GRED Web 改ざんチェック Cloud ユーザーガイド

第 15 版

（2024 年 4 月 1 日）

株式会社 日立システムズ

© Hitachi Systems, Ltd. 2024. All rights reserved.

変更履歴

Version	日付	備考
8	2020/5/20	V3.8 対応
9	2022/2/28	V3.11 対応
10	2022/5/31	機能変更対応
11	2022/8/1	GUI リニューアル対応
12	2022/9/1	V3.12 対応
13	2023/4/5	V3.13 対応
13.1	2023/6/2	V3.13.1 対応
14	2023/9/29	V3.14 対応
15	2024/4/1	V3.15 対応

© Hitachi Systems, Ltd. 2024. All rights reserved.

目次

© Hitachi Systems, Ltd. 2024. All rights reserved.

© Hitachi Systems, Ltd. 2024. All rights reserved.

1. はじめに

本書は、「GRED Web 改ざんチェック Cloud」の導入のための手順と、導入後の設定や機能について解説しております。不明点がございましたら、以下までご連絡をお願いします。
問い合わせフォーム

https://www.securebrain.co.jp/form/gredss/sbformmail.php

2. GRED Web 改ざんチェック Cloud サービス概要

「GRED Web 改ざんチェック Cloud」は、お客様の Web サイトが改ざんの被害にあっていないかを定期的に確認するサービスです。監視対象となる URL を登録するだけで、日立システムズのシステムが自動的にリンクを辿り、各ページの解析を行います。
改ざん発見時には、アラート送信と詳細なレポートを生成する機能を提供します。

2.1 検知可能な改ざん

・サイバー攻撃等による Web サイトの改ざん
・脆弱性を悪用した攻撃を行う Web サイトへの改ざん
・ウイルスなどが自動的にダウンロードされる Web サイトへの改ざん
・政治意思や思想を誇示するために意図的にページを書き換える改ざん
・ドライブバイダウンロード攻撃の踏み台に利用するための Web 改ざん
・SEO ポイゾニングによる Web 改ざん

2.2 改ざんを発見した場合

改ざんを発見した場合、管理者にアラートメールを送信します。詳細はそのメールに記載されている URL をクリックするか、管理コンソールトップページのカレンダーの赤い ⚠ のアイコンをクリックすると確認していただけます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

■詳細レポート

詳細レポートには、改ざんを検知した URL、改ざんの種類とその説明、悪質コードの脅威名とソースを表示します。このレポートにより、迅速な対応が可能になります。

2.3 改ざん検知時のページ切り替え

改ざんが見つかった場合、自動で安全なページ（GRED 内のメンテナンスページ）に切り替えることができます。この改ざん検知時のページ切り替え機能を設定しておくと、お客様の Web サイトが復旧するまで、エンドユーザーへの被害を防ぐことができます。この機能は、お客様の Web サイトが安全な状態になると表示されません。

© Hitachi Systems, Ltd. 2024. All rights reserved.

3. 管理コンソールの見方、使い方

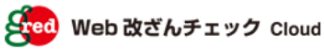
各種設定、サービスの提供は、管理コンソールより行います。

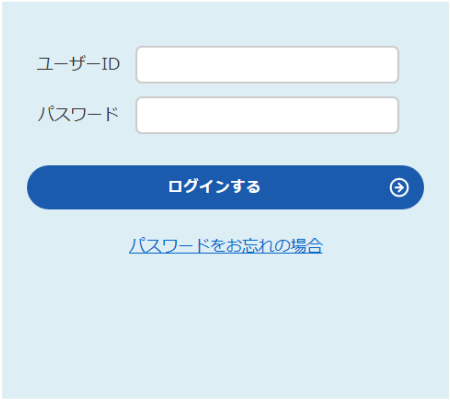
3.1 ログイン・ログアウト

ログイン

管理画面 URL にアクセスし、ログイン画面に、ID とパスワードを入力し、「ログインする」をクリックします。

初めて管理コンソールにログインするには、お客様にてパスワードを設定する必要がございます。サービス開始後に送付される登録通知メールの手順に従い、パスワードを設定してください。パスワード設定後、パスワード設定完了の通知が届きますので、メールに記載しているログイン画面 URL よりログインして下さい。





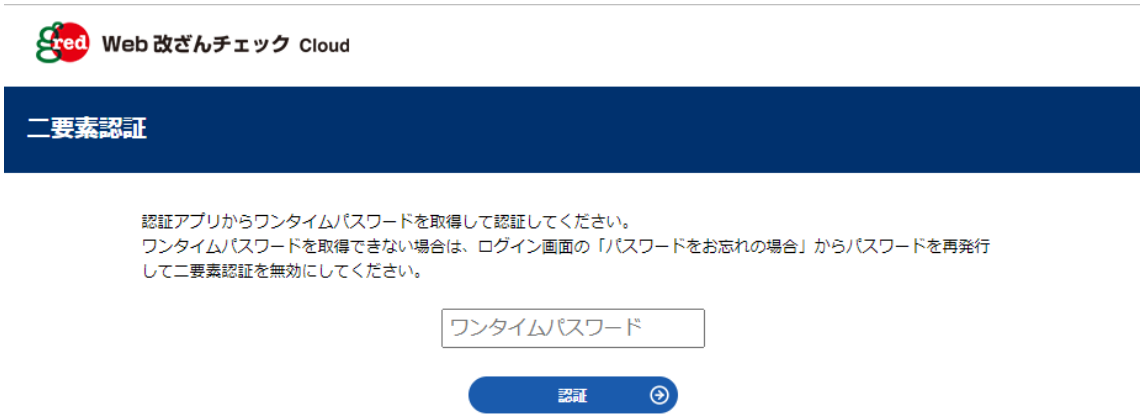
システムメンテナンスや障害の詳細情報はログイン後に確認いただけます。

詳細は「3.10 お知らせ機能」を参照してください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

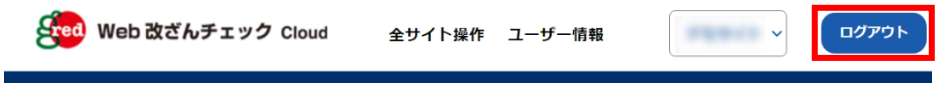
二要素認証

二要素認証を有効に設定することでIDとパスワードでの認証後にワンタイムパスワードを使用した二要素認証をします。スマートフォンにインストールした認証アプリからワンタイムパスワードを取得することでログインしてください。認証アプリは Google Authenticator または Microsoft Authenticator を利用してください。二要素認証の設定方法については「5.2 ユーザー情報の確認・変更」を参照してください。



ログアウト

ヘッダーの右上にある『ログアウト』ボタンをクリックすると、ログアウトされます。



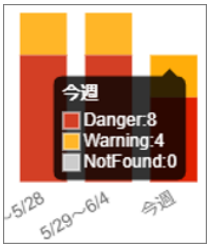
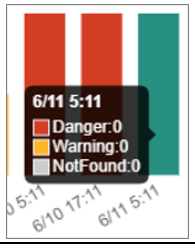
© Hitachi Systems, Ltd. 2024. All rights reserved.

3.2 ダッシュボード画面

正しくログインが完了すると、ダッシュボード画面へ遷移します。ダッシュボード画面では、最新の解析結果と過去の解析結果の統計情報（直近、ウィークリー、マンスリー）の棒グラフと解析履歴（1 年分）をカレンダーで表示します。

	項目名	内容
①	最終結果	最新の解析結果を表示します。詳細は 3.3 以降の「解析結果表示」参照して下さい。
②	本日の解析結果履歴	最新の解析結果を表示します。
③	直近の解析結果	直近の 8 回分の解析結果（解析毎の検知数の累計）を棒グラフで表示します。
④	ウィークリーの解析結果	今週を含めて 8 週間分の解析結果の累計を一週間ごとの棒グラフで表示します。
⑤	マンスリーの解析結果	今月を含めて 8 か月分解析結果の累計を一か月ごとの棒グラフで表示します。
⑥	解析結果カレンダー	解析の結果を、それぞれ安全、警告、危険のマークをカレンダー上に表示します。カレンダー上部の「期間を選択」リストボックスで表示する年月の切り替えが出来ます。
⑦	解析サイトリスト	解析サイトが複数ある場合にはリストで表示されます。リストボックスに表示される解析サイトを選択すると表示対象の解析サイトの切り替えが出来ます。
⑧	詳細設定ボタン	各解析サイトの解析履歴、詳細設定画面に遷移します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

⑨	ツールチップ	各棒グラフにカーソルを合わせると解析結果の検知数が表示されます。 改ざん検知された場合  改ざん検知が無い場合 
⑩	ログイン履歴	前回のログイン日時を表示します。右側の「履歴」をクリックすると過去のログイン履歴を表示するページに遷移します。詳細は 6.11 の「ログイン履歴確認機能」を参照して下さい。
⑪	お知らせ	管理画面には最新のお知らせが表示されます。「一覧を見る」をクリックすると過去のお知らせを確認することができます。詳細は 3.10 の「お知らせ機能」を参照してください。

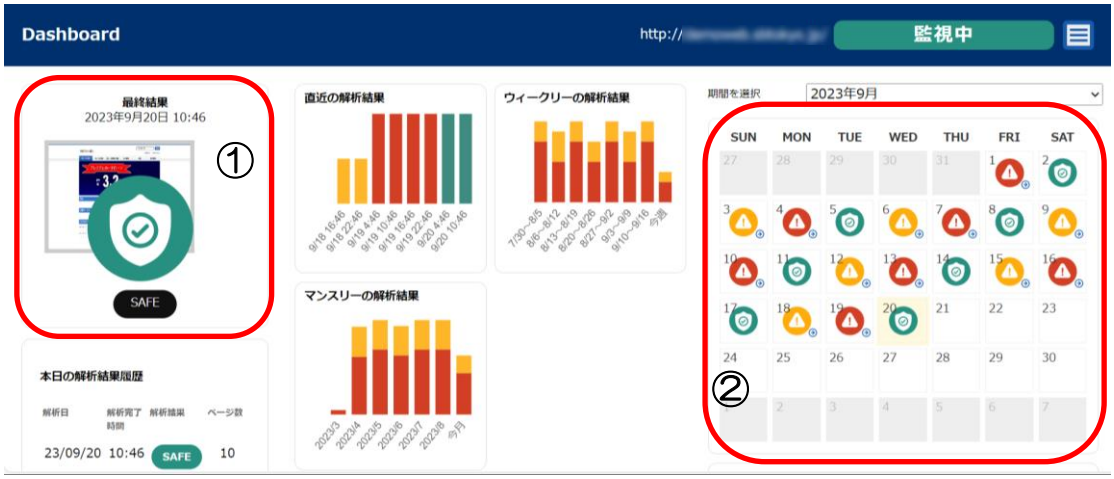
※アイコンと棒グラフの色について

（詳細は 3.3 以降の「解析結果表示」参照して下さい。）

© Hitachi Systems, Ltd. 2024. All rights reserved.

3.3 解析結果表示 緑（SAFE・安全）

解析した結果、安全なサイトであると判定された場合、画面には「SAFE」と緑で表示されます。



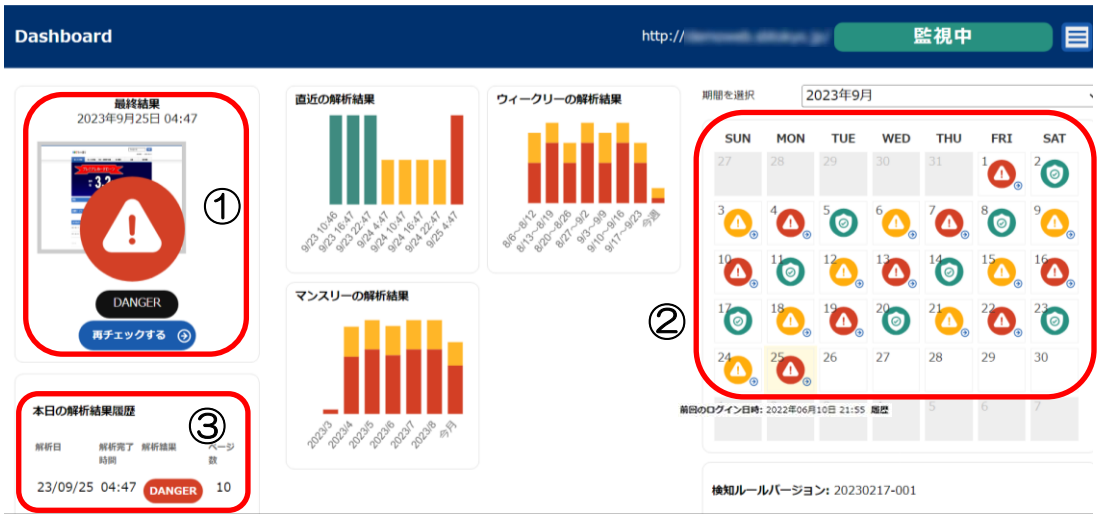
「SAFE」表示内容

	項目名	内容
①	判定結果	安全なサイトであることを示す「SAFE」が表示されます。
②	解析結果カレンダー	解析の結果、安全なサイトと判断された場合には緑色の  マークをカレンダー上に表示します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

3.4 解析結果表示　赤（DANGER・危険）

解析を行った結果、危険なサイトであると判定された場合、画面には赤の  マークが表示されます。

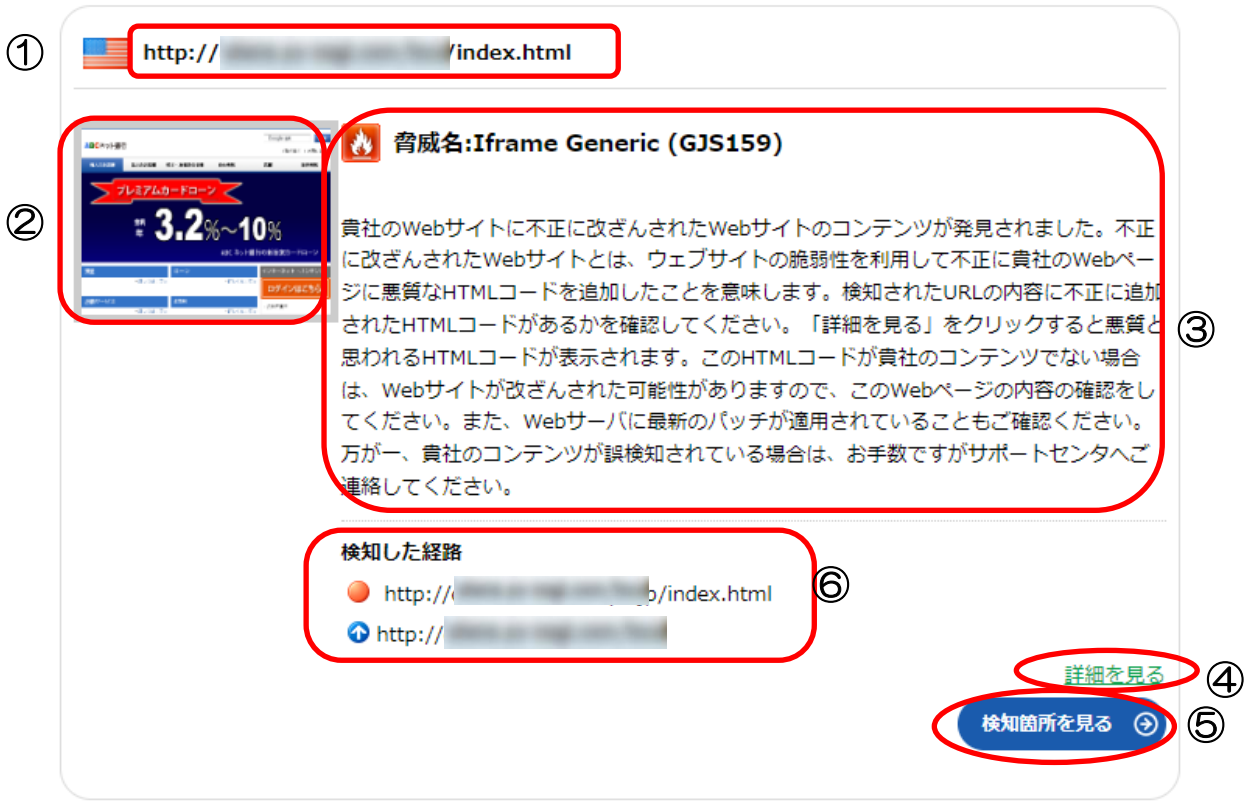


「DANGER」表示内容

	項目名	内容
①	判定結果	危険なサイトであることを示す赤い  が表示されます。
②	解析結果カレンダー	解析の結果、危険なサイトと判断された場合には赤色の  マークをカレンダー上に表示します。  のマークをクリックすると、解析結果の内容を表示することができます。
③	最新の解析結果	最新の解析結果を表示します。危険なサイトだと判断された場合には赤く表示され、解析結果には危険の内容が表示されます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

解析結果カレンダーの  をクリックすると、解析結果の内容が表示されます。



解析結果の表示内容

	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。
④	解析結果の詳細	問題のあるソースコードがハイライト表示されます。
⑤	検知した箇所を見る	検知箇所が可視化されます。
⑥	検知した経路	検知した箇所の経路が表示されます。 「脅威名」の名称が表示されている場合には、検知経路が表示されます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

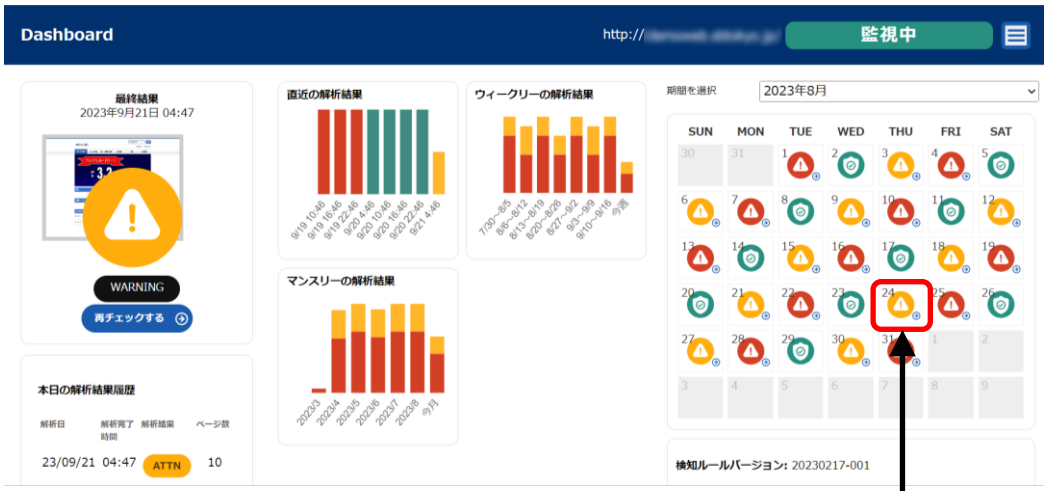
また、詳細レポートの「詳細を見る」をクリックすると、改ざんを検知したページのソースコードが表示され、問題のある箇所をハイライト表示します。

問題が見つかりました

© Hitachi Systems, Ltd. 2024. All rights reserved.

3.5 解析結果表示 黄色（Warning・警告）クロスドメインスクリプト検知

許可設定をしていないクロスドメインスクリプトを検知すると、管理コンソールホームのマークが黄色の「Warning」(警告)に変化します。

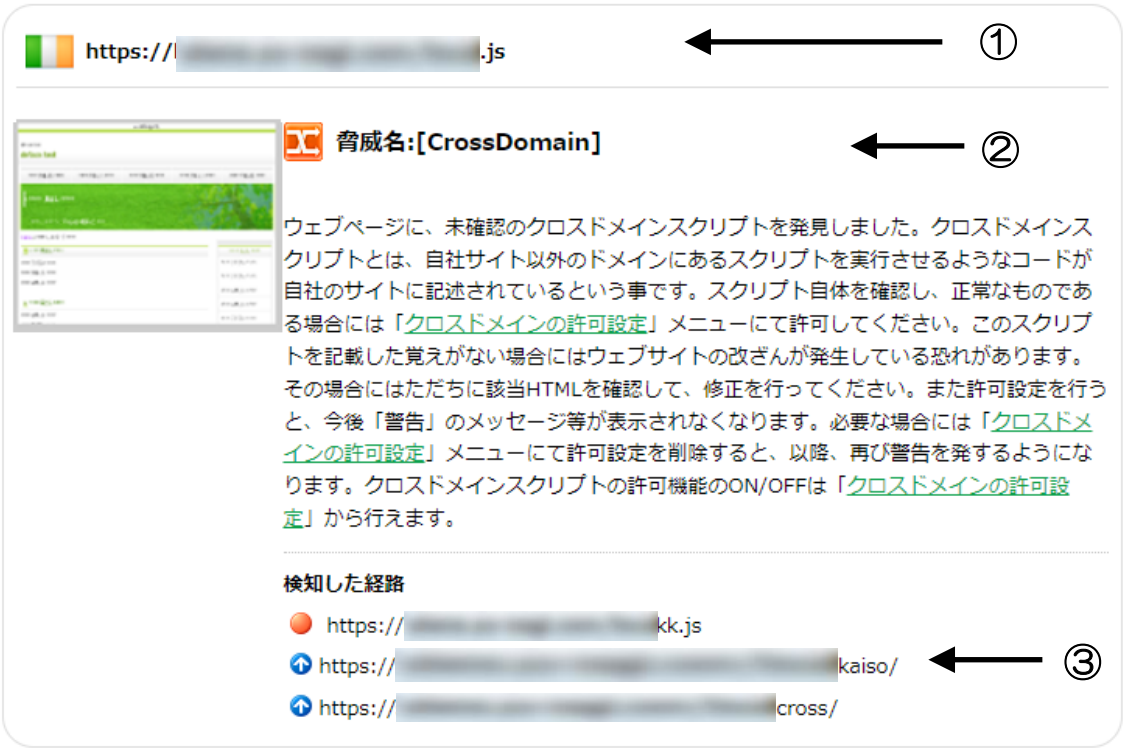


黄色のマークをクリックすると
詳細ページが表示されます。

■詳細ページ

注意が必要です

2022年5月4日 10:03



© Hitachi Systems, Ltd. 2024. All rights reserved.

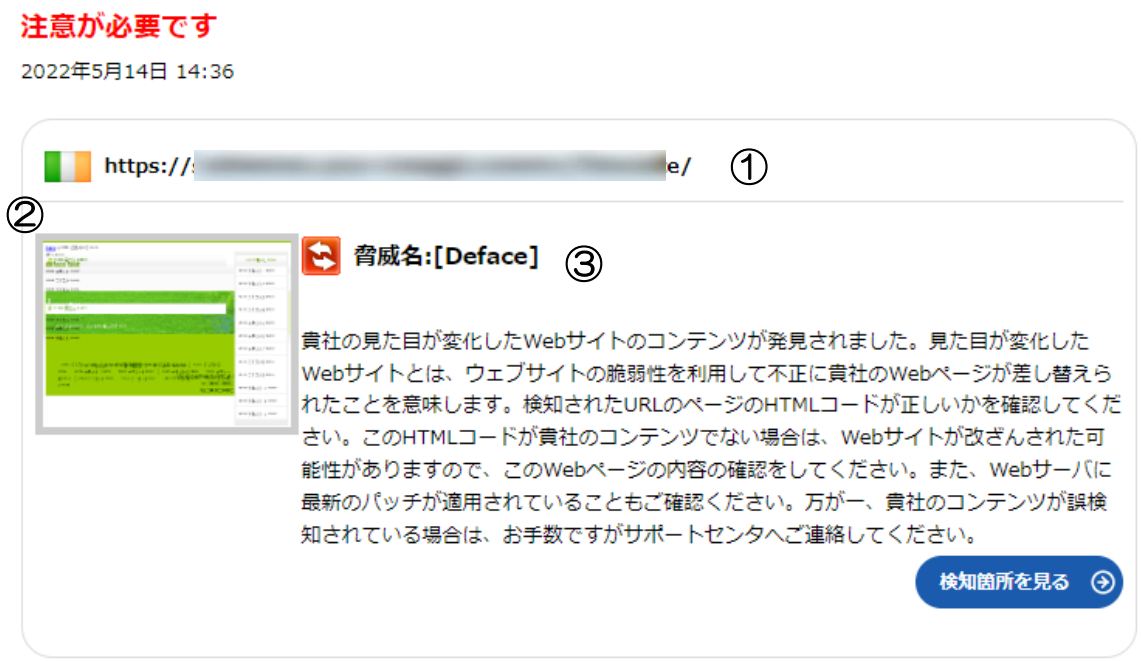
解析結果の表示内容

	項目名	内容
①	URL 表示	クロスドメインを検知した URL が表示されます。
②	解析結果	クロスドメインの許可設定の説明
③	クロスドメインの経路	クロスドメインが見つかった経路を表示します。

「クロスドメインの許可設定」から自社のドメイン以外に利用しているスクリプトのドメインを設定しておくことによって、解析結果の「Waning」表示を「SAFE」に変更します。（設定の方法は、「5.7 クロスドメインの許可設定」をご覧ください。）

3.6 解析結果表示 黄色（Warning・警告）TOP ページの見た目変化検知

Top ページのコンテンツが著しく変化した場合に、検知メールが送信され詳細を管理コンソールで確認することができます。
※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

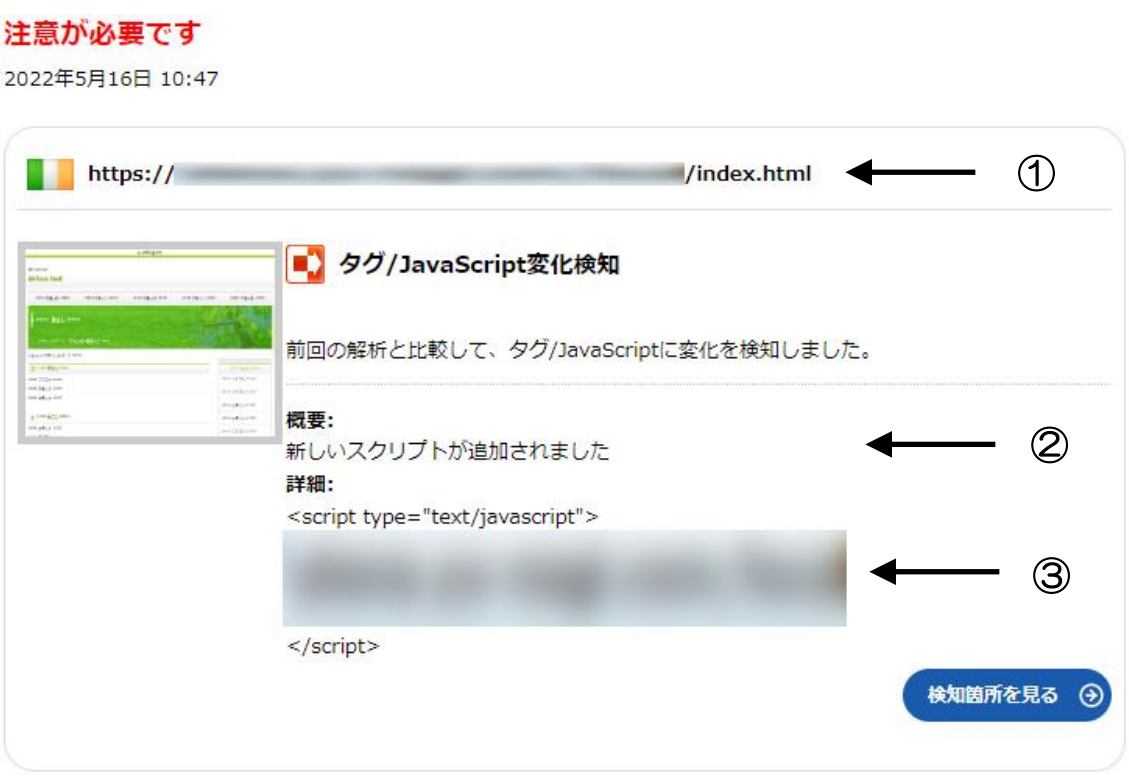


	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

3.7 解析結果表示 黄色（Warning・警告）タグ・JavaScript の変化検知

JavaScript の変化を見ることにより改ざんを検知する「スクリプト変化検知エンジン」と HTML 内の特定タグの src 属性や href 属性変化を検知する「リンクタグ変化検知エンジン」を実装しました。「タグ/JavaScript 変化検知」という項目で表示されます。詳細は管理コンソールで確認することができます。



	項目名	内容
①	URL 表示	タグ/JavaScript の変化を検知した URL が表示されます。
②	概要	タグ/JavaScript の変化の概要
③	変化したタグ/JavaScript	変化したソースコードを表示します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

3.8 解析結果表示 黄色（Warning・警告）EXE 解析検知

監視対象ページにある実行ファイルが、マルウェアと類似した動きをしている場合に警告を行う「表層解析エンジン」を実装しました。検知メールが送信され詳細を管理コンソールで確認することができます。

※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	概要	ファイルの概要
③	解析結果	挙動の詳細を表示します。

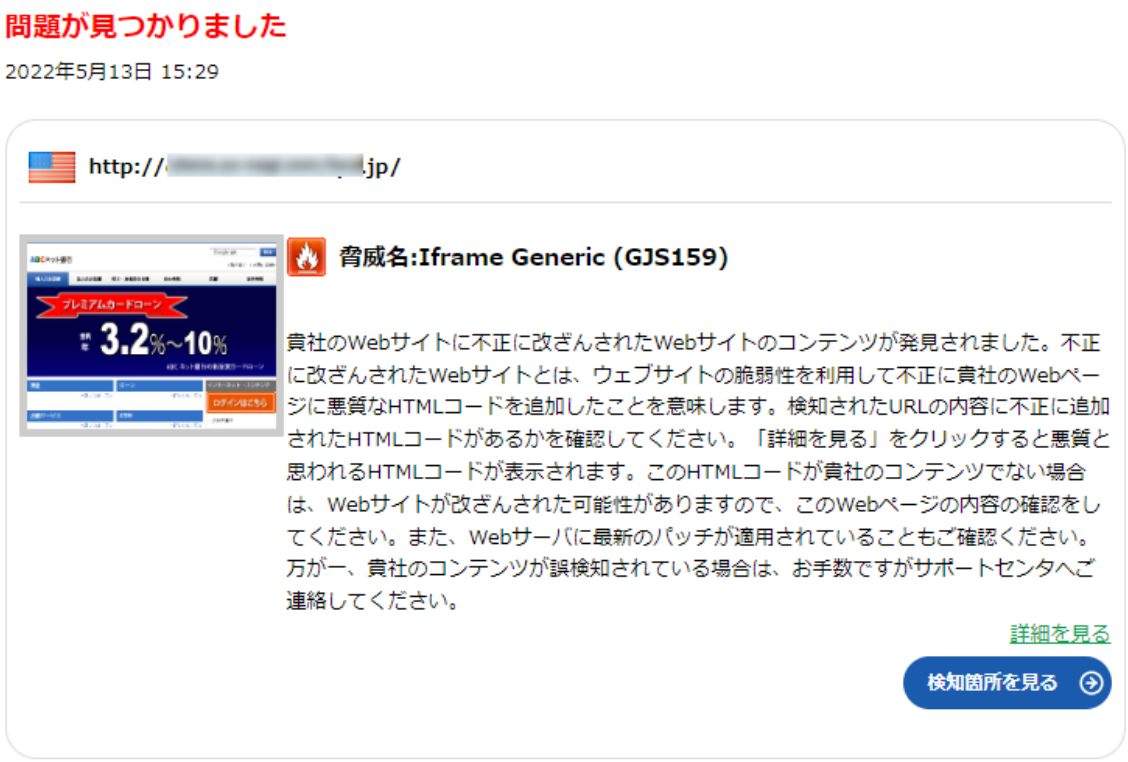
© Hitachi Systems, Ltd. 2024. All rights reserved.

3.9 改ざん検知時のメール送信

危険なサイトを検知すると、管理コンソールのアイコンが赤または黄色に変わると同時に登録いただいたメールアドレスに解析結果が送信されます。

メール本文には、検知したページの URL と内容が表示されます。
メール本文のリンクをクリックすると詳細ページにジャンプします。改ざんされている可能性があるウェブページの参照には十分ご注意の上、確認してください。
※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

■詳細ページ



改ざん検知以外のアラートメールは以下 5 種です。詳細は巻末の「付録 アラートメールサンプル」をご参照ください。
なおアラートメールは、管理コンソールから「メールを送信する」、「送信しない」を選択することができます。

・Top ページのヘルスチェック検知時
・見た目変化検知時
・クロスドメインスクリプト検知時
・EXE 解析検知時
・タグ・JavaScript 変化検知時

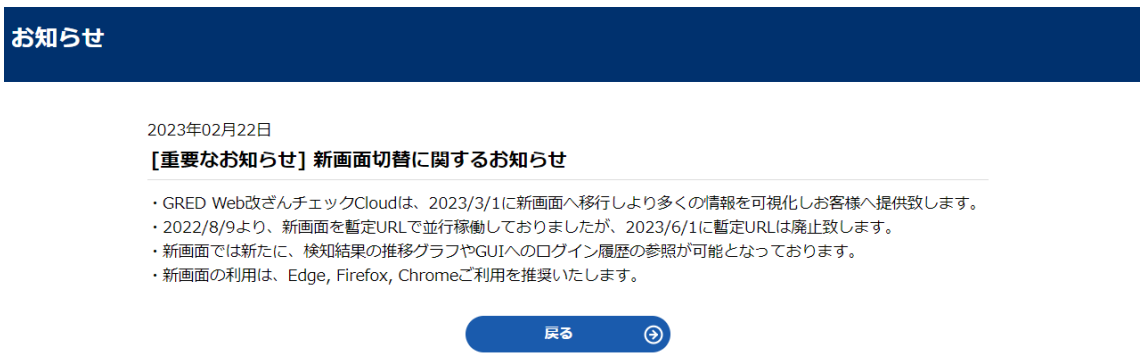
© Hitachi Systems, Ltd. 2024. All rights reserved.

3.10 お知らせ機能

Gred Web 改ざんチェックからのお知らせやメンテナンスなどの情報を確認することができます。
管理画面には最新のお知らせが一件表示されます。タイトルをクリックすると詳細画面へ遷移します。
「一覧を見る：」をクリックすると、過去のお知らせ一覧が確認できます。

■一覧ページ

■詳細ページ



お知らせはメールでも受け取ることができます。
設定方法は「5.2 ユーザー情報の確認・変更」を参照してください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

4. 解析履歴

解析履歴やレポートの確認方法をご説明します。

4.1 解析履歴

過去の解析を確認することができます。

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

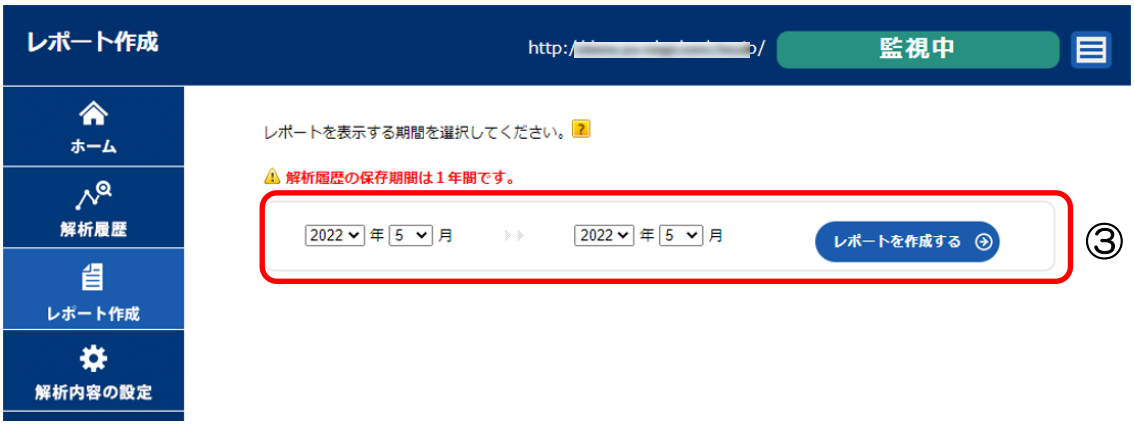
② 左側の「**解析履歴**」をクリックします。

③ 解析日、解析完了時間、解析結果、ページ数を新しいものから順に表示します。赤、黄色の項目はクリックすると詳細ページにジャンプします。
「**ダウンロード**」をクリックする事で、CSV 形式のファイルでダウンロード可能です。

© Hitachi Systems, Ltd. 2024. All rights reserved.

4.2 レポート作成

左側にある「レポート作成」をクリックします。
一定期間の解析結果の統計情報を見ることができます。

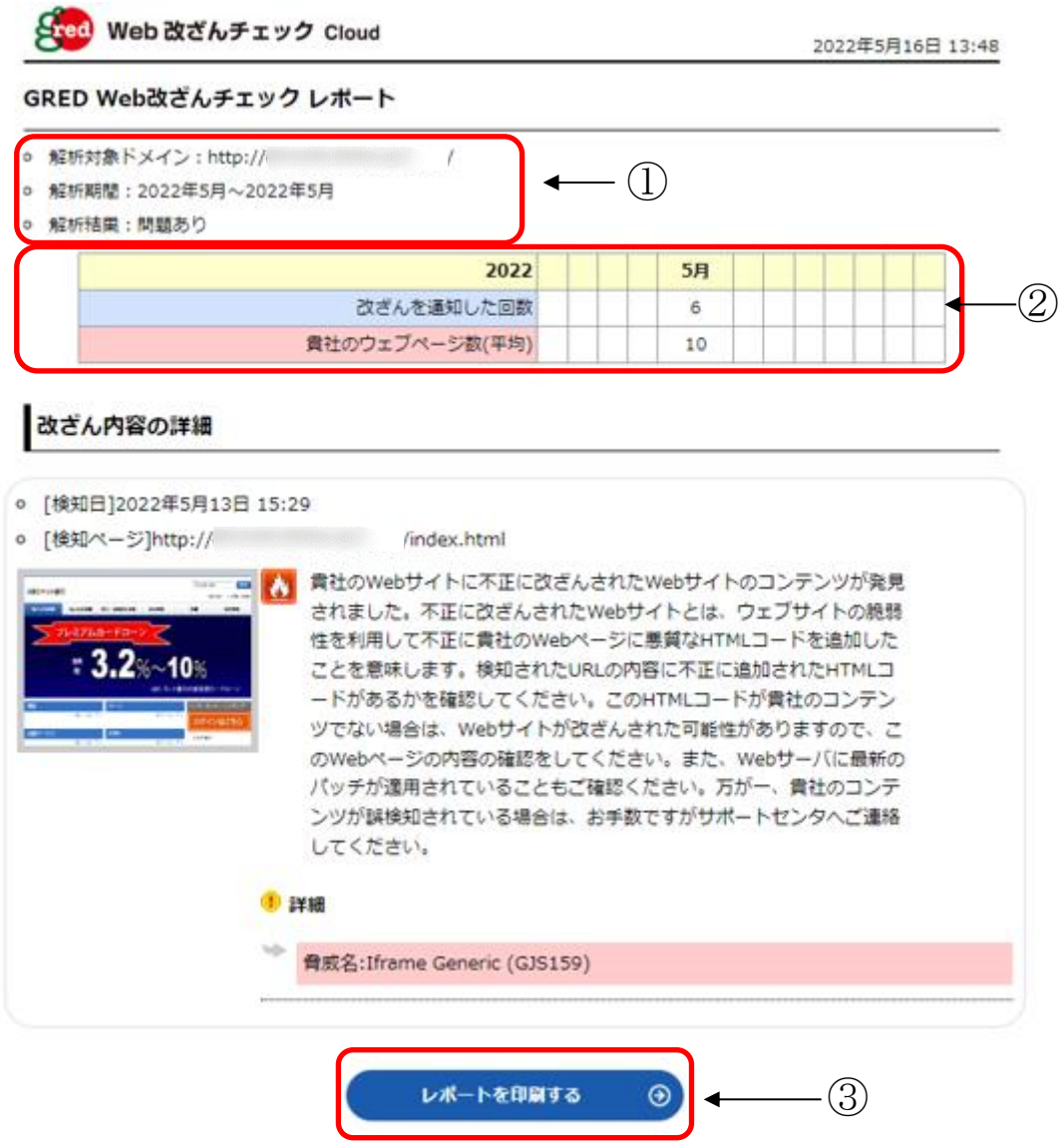


① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 左側の「**レポート作成**」をクリックします。

③ 統計を出したい期間（1 か月単位）を指定し「**レポートを作成する**」ボタンをクリックすると、指定された期間の統計概要と月ごとの解析結果が表示されます。

© Hitachi Systems, Ltd. 2024. All rights reserved.



	項目名	内容
①	統計概要	解析したサイトと期間、解析結果
②	統計詳細	月別の統計結果
③	印刷	レポートを印刷します。

4.3 週間レポートメール

週に１度（月曜日）に、１週間の解析結果をメールでお知らせします。

※メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5. 各種設定

各種機能の追加・変更等の設定方法をご説明します。

5.1 ユーザー管理

新しいユーザー（サブユーザー）を追加します。 管理画面へアクセスが可能なユーザーを 5 名まで追加登録できます。申込時に登録したメインユーザーのみサブユーザーの登録が可能です。

① ヘッダーの「**ユーザー情報**」をクリックします。

② 「**サブユーザー**」をクリックします。

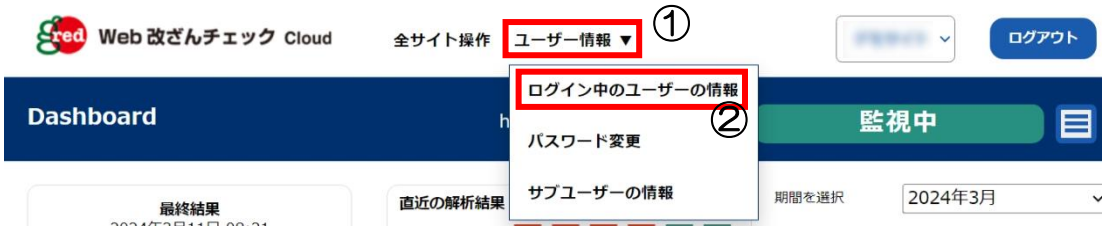
③ サブユーザーご担当者名（お名前）、ログイン ID、アラート用メールアドレス、アラートメールの受け取りの有無、使用言語（日本語/英語）、タイムゾーン、アクセスの権限を入力し、「**追加する**」をクリックします。

※ログイン ID は一度設定しますと変更はできませんのでご注意ください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.2 ユーザー情報の確認・変更

アラート用メールアドレス、名前の変更が行えます。
また、週間レポートメール、アラートメールの受け取りの有無、使用言語（日本語/英語）、タイムゾーン、二要素認証もここで変更できます。



© Hitachi Systems, Ltd. 2024. All rights reserved.

① ヘッダーの「**ユーザー情報**」をクリックします。

② 「**ログイン中のユーザーの情報**」をクリックします。

③ 設定変更などを行い、「**確認する**」をクリックします。

※「お知らせ通知」は申込時に登録したメインユーザーのみ設定できます。

④ 確認画面にて変更内容を確認し、「**変更する**」をクリックします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

二要素認証を無効から有効へ変更すると以下の画面を表示します。

こちらの画面で QR コードまたは登録用コードを使用して認証アプリ（Google Authenticator または Microsoft Authenticator）へ登録してください。次回以降のログイン時には、ID とパスワードに加えて認証アプリで取得するワンタイムパスワードを使用してログインしてください。

認証アプリへ登録せずにログアウトした場合は、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。 認証アプリの削除やデバイスの変更・紛失等によりログインできなくなった場合も、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.3 パスワードの変更

ログインパスワードの変更は、ここから行ってください。

① ヘッダーの「**ユーザー情報**」をクリックします。

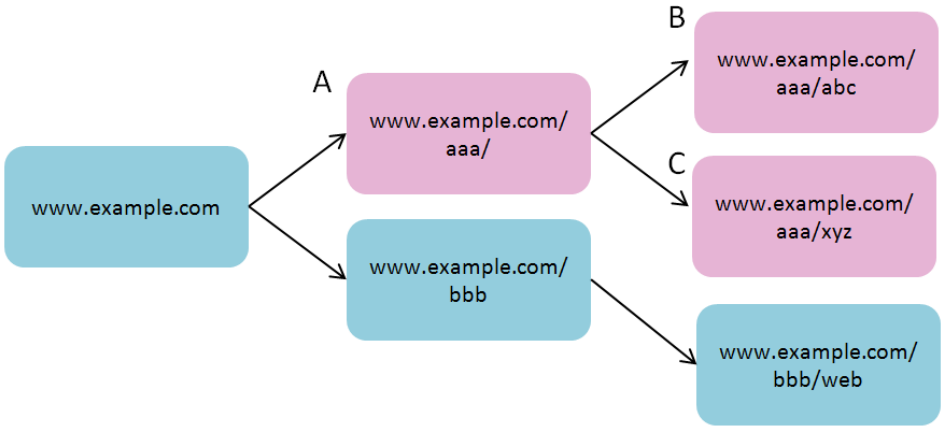
② 「**パスワード変更**」をクリックします。

③ 現在のパスワードと新しいパスワードを入力し、「**変更する**」をクリックします。

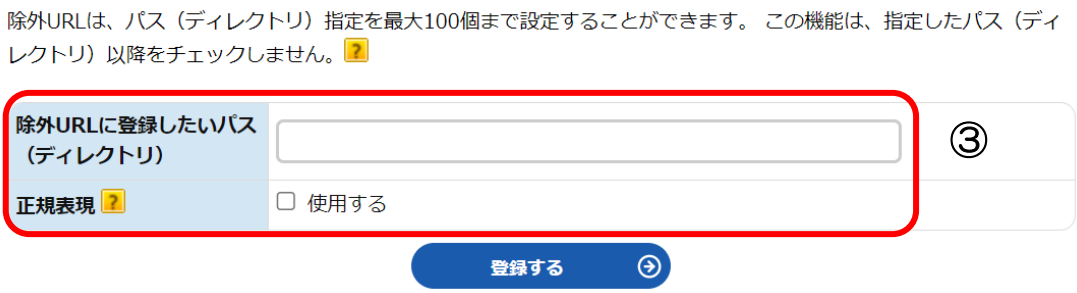
© Hitachi Systems, Ltd. 2024. All rights reserved.

5.4 除外 URL の登録

除外 URL の設定は、パス（ディレクトリ）指定を最大 100 個まで行う事ができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。



※A(www.example.com/aaa/)を指定した場合、**B** と **C** も解析対象から除外されます。



① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 画面中央のメニューから「**除外設定**」内の「**除外 URL**」をクリックします。

③ 「**除外 URL に登録したいパス（ディレクトリ）**」欄に任意の URL もしくは正規表現を入力し「**登録する**」をクリックします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

※除外したい URL については、正規表現を使用することも可能です。正規表現を使用したい場合は、「正規表現」にチェックを入れて登録してください。

■記述例

設定	効果
www.foo.bar	www.foo.bar で終わるドメインの URL をクロールしない。 例)次の URL はクロールしません http://www.foo.bar/top.html http://www.foo.bar/map.html http://ex1.www.foo.bar/
foo.bar	foo.bar で終わるドメインの URL をクロールしない。 例)次の URL はクロールしません http://foo.bar/top.html http://www.foo.bar/ http://blog.foo.bar/user1/entry.html
www.foo.bar/blog	www.foo.bar で終わるドメインの/blog で始まるパスの URL をクロールしない。 例)次の URL はクロールしません http://www.foo.bar/blog/ http://www.foo.bar/blog/entry/1.html

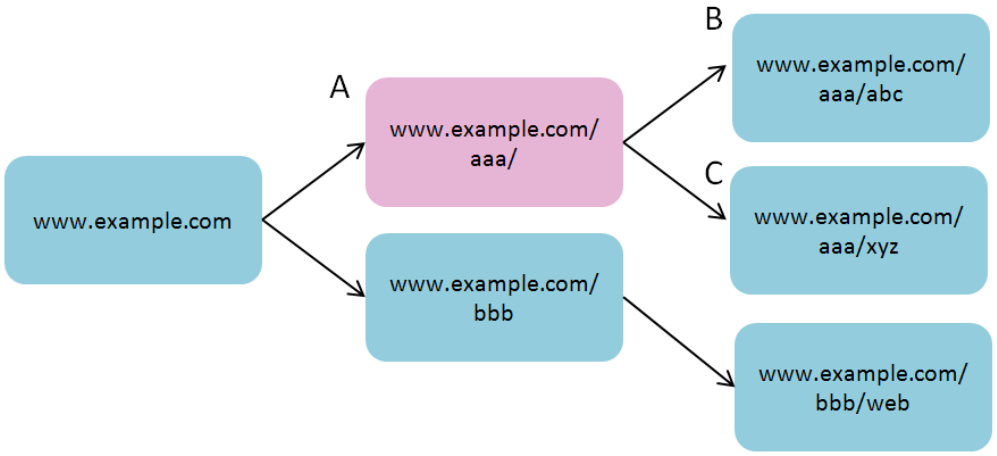
■正規表現を使用する場合の記述例

設定	効果
www¥.foo¥.bar/.*/blog/	ドメインが www.foo.bar で終わり、2 つ目以降のディレクトリが blog である URL を除外する。 例)次の URL はクロールしません https://www.foo.bar/aaa/blog/index.html https://www.foo.bar/bbb/blog/index.html 注意点 *(アスタリスク)はワイルドカードではなく正規表現になる為、上記のように任意のディレクトリを除外する際は*のみの指定では除外出来ません。 .(ドット)は正規表現では任意の 1 文字として扱われますので、正規表現として扱わない場合は、¥(エスケープ)を付加してください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.5 ホワイトリストの登録

ホワイトリストは、あらかじめ問題が無い事がわかっている URL を指定して、常に「OK」という判断を行うリストです。最大 10 個まで指定することが可能です。
このリストに指定した URL は解析ページ数としてカウントされますが必ず「OK」という結果になります。ページにリンクがあった場合にはそのリンクから先もクローリングします。ただし、このリストに指定したページのみ「OK」となる事に注意してください。



※A(www.example.com/aaa/)を指定した場合、このページは必ず「OK」という解析結果となります。 B と C は通常通り解析が行われます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。
② 画面中央のメニューから「**除外設定**」内の「**ホワイトリスト**」をクリックします。
③ 「**ホワイトリストに登録したい URL**」欄に任意の URL を入力し「**登録する**」をクリックします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.6 監視の ON/OFF とウェブ解析対象階層の指定

GRED Web 改ざんチェック Cloud 自体の監視の ON/OFF を管理コンソールで行うことができます。また、解析対象の階層数を指定する事により、解析ページ数の調整が可能です。指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。

監視の ON/OFF の設定

① 画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 画面中央のメニューから「基本設定」内の「**監視の ON/OFF と基本設定**」をクリックします。

③ 有効または、無効にチェックを入れて「**変更する**」ボタンをクリックします。

④ 「ウェブ解析対象階層の指定」欄に解析対象の階層数を入力し「**変更する**」をクリックします。

⑤ 検知するレベル「**スクリプトタグに変化がある場合に検知**」、「**特定のタグに変化がある場合に検知（スクリプトタグ含む）**」、「**無効**」のいずれかを選択し「**変更する**」ボタンをクリックします。

※デフォルトでは「スクリプトタグに変化がある場合に検知」がオンになっています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.7 クロスドメインの許可設定

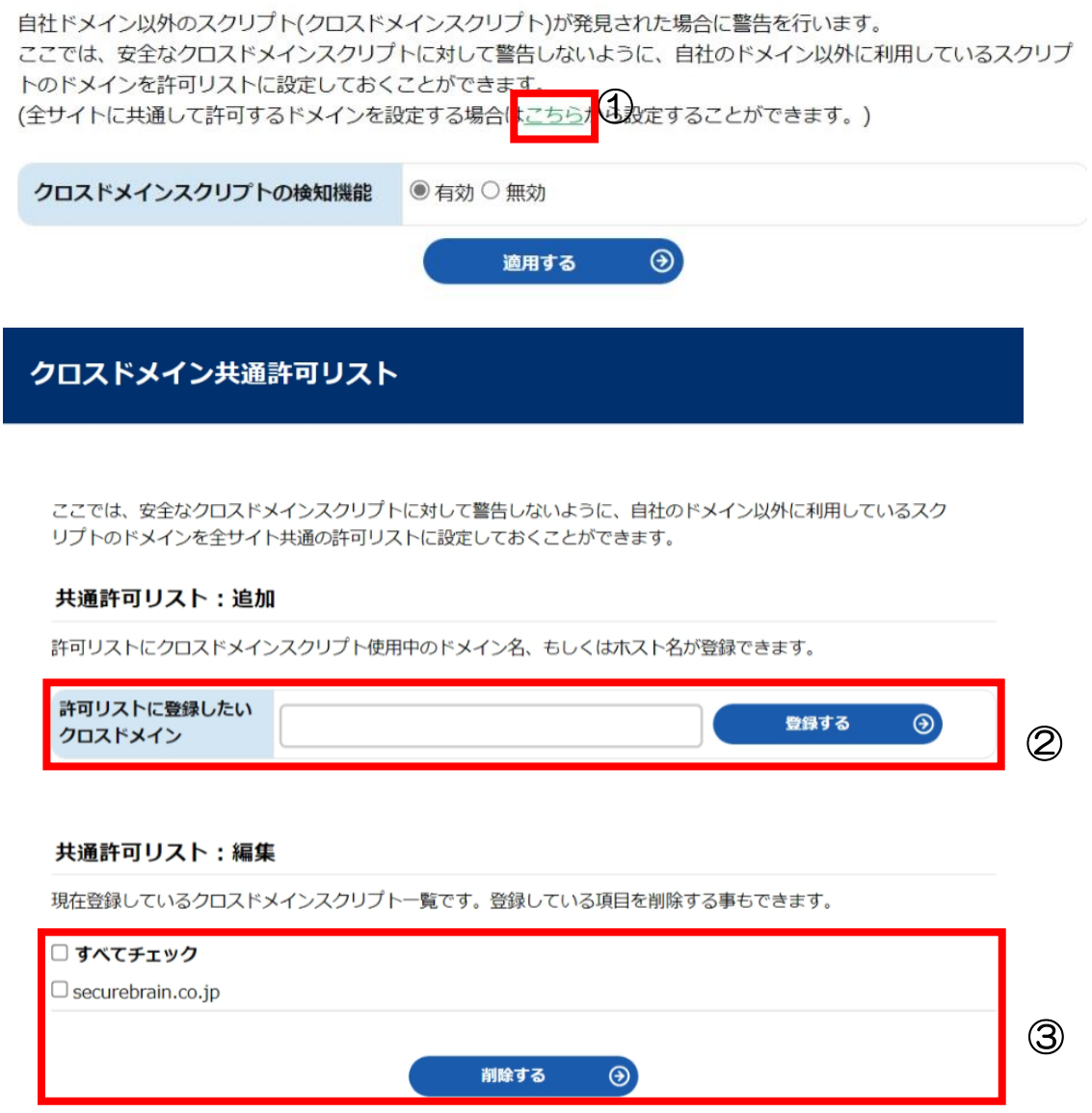
ウェブ改ざんチェックの「クロスドメインスクリプト管理・警告機能」 は、自社サイト外に誘導するスクリプトがウェブページに埋め込まれた場合に「警告」を行います。あらかじめ任意で埋め込んだ外部に飛ばすスクリプトは、許可リストに登録してください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

① 画面左上の  をクリックし、「**解析内容の設定**」に遷移します。
② 画面中央のメニューから「**クロスドメイン設定**」内の「**クロスドメイン検知**」をクリックします。
③ クロスドメインスクリプトの「**有効/無効**」の設定ができます。いずれかにチェックを入れます。
④ 「**許可リスト：クイック登録**」では見つかったクロスドメインスクリプトが表示されます。許可する場合は、ボックスにチェックを入れて「**登録する**」ボタンをクリックしてください。
⑤ 「**許可リスト：編集**」では登録している項目を削除することもできます。
削除したい URL のチェックボックスにチェックを入れ、「**削除する**」ボタンをクリックします。

・クロスドメイン共通許可リスト

全サイトに共通しているクロスドメインを許可リストに登録することができます。



© Hitachi Systems, Ltd. 2024. All rights reserved.

① 「**こちら**」をクリックします。
② 「**共通許可リスト：追加**」に URL・ドメインを入力し「**登録する**」ボタンをクリックします。
③ 「**共通許可リスト：編集**」では登録している項目を削除することができます。削除したい URL・ドメインにチェックを入れ「**削除する**」ボタンをクリックします。

クロスドメイン共通許可リストの設定画面はヘッダーからもアクセスが可能です。

① ヘッダーの「**全サイト操作**」をクリックします。
② 「**クロスドメイン共通許可リスト**」をクリックします。
③ クロスドメイン共通許可リストの設定画面に遷移します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.8 改ざん検知時のページ切り替え機能の設定

改ざんが確認された場合に、自動でページを切り替える機能が利用できます。

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。

② 画面中央のメニューから「**オプション**」内の「**改ざん時切り替え機能**」をクリックします。

③ お客様専用のタグが生成されます。<html>タグのすぐ後に取得したタグを挿入して下さい。

■タグのサンプル　※切り替え機能のタグはお客様ごとに異なります。

```
<script type="text/javascript" src="https://www3.gred.jp/saas/gred_checker.js?sid=[redacted]">
</script>
```

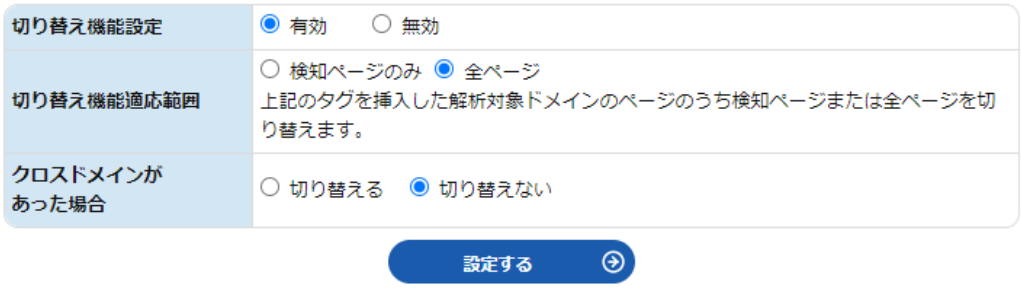
お客様独自のメンテナンスページを表示させる場合には末尾に【&redirect_url=”挿入したいメンテナンスページの URL “】を追加してください。

・切り替え機能設定

ページ切り替え機能の有効/無効を設定します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

「有効」を選択すると切り替えに関するオプションが表示されます。



・切換え画面サンプル

※ウェブ改ざんチェックのサービスを終了した場合は、埋め込んだタグの削除をお願いします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.9 GRED 証明書の設定

サイトが改ざんされていないことを証明できる「GRED 証明書」が利用できます。この証明書をサイトに表示し、クリックすると検証結果が表示されます。

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。
② 画面中央のメニューから「**オプション**」内の「**GRED 証明書**」をクリックします。
③ お客様専用のタグが生成されます。そのタグをページ内の GRED 証明書を表示させたい部分に挿入して下さい。

■タグのサンプル※GRED 証明書のタグはお客様ごとに異なります。

```
<a href="https://www2.gred.jp/saas/ratingVerify.htm?sid=
onclick="window.open('https://www2.gred.jp/saas/ratingVerify.htm?sid=',
'_blank', 'width=600,height=600,resizable=no,menubar=yes,toolbar=yes');
return false;" oncontextmenu="alert('この画像はコピーできません。');return
false;"><img height="40" border="0" width="85" src="https://www2.gred.jp
/saas/seal.gif?sid=" onerror = "javascript:src = 'https://www.gred.jp
```

gred証明書の検証ページを見る

© Hitachi Systems, Ltd. 2024. All rights reserved.

表示内容

Web サイト名:

最終解析完了時間:

（最後にチェックした時間が表示されます）

解析結果:

（最後に解析を行った結果が表示されます ）

※GRED Web 改ざんチェック Cloud のサービスを終了した場合は、埋め込んだタグの削除をお願いします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5.10 非リンク URL の登録

TOP の URL から辿れない URL を管理画面から非リンク URL として登録することで解析対象にすることができます。登録できる非リンク URL は、解析対象ドメインのみとなります。自動的にリンクを辿らないため、解析対象とする URL を 1 件ずつ登録する必要があります。最大 20 件まで登録出来ます。ご契約されている URL 数の範囲内で TOP からリンクされている URL と、このページで登録した非リンク URL を解析します。TOP からリンクされている URL の解析終了後に非リンク URL を解析します。解析中に契約されている URL 数を超えた場合は、その時点で解析を終了します。

なお、本設定で登録した URL は、「6.6 リンク切れ検知機能」「6.7 リンク構造可視化機能」の対象外となります。

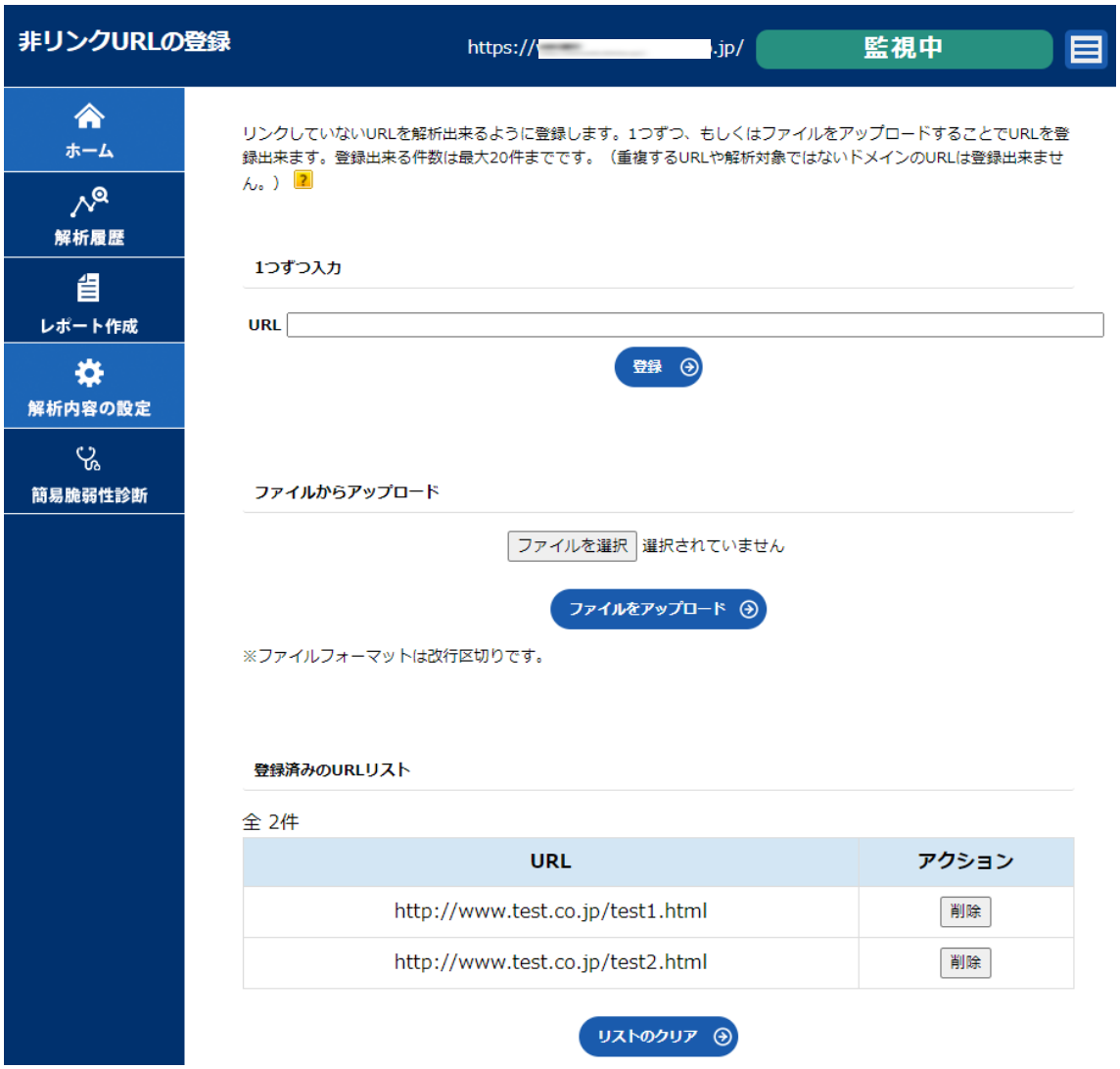
非リンク URL 登録画面表示方法

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します

② 「オプション」メニューから「非リンク URL の登録」をクリックします。

③ 非リンク URL の登録画面が表示されます。

© Hitachi Systems, Ltd. 2024. All rights reserved.



非リンク URL の登録方法（二通り）

① URL を一つずつ登録する

URL 入力ボックスに URL を入力し「登録」ボタンをクリックしてください。下部の登録済みの URL リストに追加されます。

② ファイルからアップロードする

「ファイルを選択」ボタンから改行区切りの URL リストを選択し「ファイルをアップロード」ボタンをクリックしてください。下部の登録済みの URL リストに追加されます。

非リンク URL の削除方法（二通り）

① 削除ボタンから一つずつ削除する

登録済み URL リストのアクション項目にある削除ボタンをクリックします。該当の URL がリストから削除されます。

② 一括削除する

登録済み URL リストの下部にある「リストのクリア」ボタンをクリックします。リストからすべての URL が削除されます。

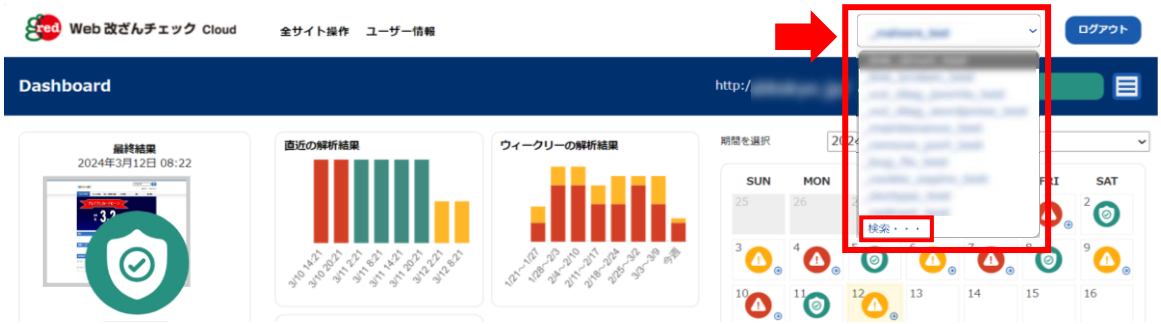
© Hitachi Systems, Ltd. 2024. All rights reserved.

6. その他の機能・サービス

各種設定、サービスの提供は、管理コンソールより行います。

6.1 解析サイトの検索

複数の解析サイトを 1 つの管理コンソールで管理している場合、確認したい解析サイトの検索ができます。解析サイトが 10 以上ある場合に「検索・・・」リンクが表示され、クリックすると該当する解析サイトの管理コンソールへのリンク一覧が表示されます。



ヘッダーの「全サイト操作」をクリックし「サイト検索」からアクセスも可能です。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.2 オンデマンドチェック機能

改ざんを検知し、修復を行った際に、問題がないか確認できるよう、即時チェックを行う機能です。1 日に 2 回まで使用可能です。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.3 GRED 証明書

この証明書をお客様のサイトに表示すれば、GRED によって守られている検証結果を表示させることが出来ます。HTML の img タグにより GRED 証明書のイメージを埋めこみます。タグをページ内の GRED 証明書を表示させたい部分に挿入して下さい。エンドユーザーが GRED 証明書をクリックすると、ポップアップ画面が表示され、そのページについて GRED での解析結果が表示されます。
GRED 証明書のタグの入手方法は「GRED 証明書の設定」をご覧ください。

クリックすると以下の画面が開きます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.4 ポートスキャン診断機能

ポートスキャン診断は、ポートスキャン診断を選択し診断実行ボタンをクリックするだけで、対象のポートが開いているか閉じているかを調査します。開いているポートに脆弱性情報が提供されている製品がある場合は、情報を提供しているウェブサイトの URL 等、参照情報を表示します。

ポートスキャン診断は以下のポートに対して診断を実施します。

診断ポート：20-22、53、80、443、445、1433、3306、8080、8887、10001、20001、30001、40001、50001、60001

【使用方法】

© Hitachi Systems, Ltd. 2024. All rights reserved.

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。
② 左側の「**簡易脆弱性診断**」をクリックします。
③ 「**ポートスキャン診断**」にチェックを入れます。
④ 「**診断実行**」をクリックします。
⑤ 診断完了後、ポートスキャン診断結果のタブに結果が表示されます。

【ご注意事項】
※１）本診断の特性上、不正アクセス検知システム（サーバ監視ツールや、IPS/Firewall など）に不正なアクセスとして検知される可能性がございます。診断を行う際は、事前に関連部署に対して脆弱性診断実施の了承、並びに本脆弱性診断サービスからのアクセスを一時的に監視対象から外していただく等のご対応をお願いいたします。「診断実行」ボタンをクリックすると上記注意事項が書かれたポップアップが表示され、注意書きに同意をいただいた上でスキャンを開始する仕様になっています。本ツールの IP アドレスを確認したい場合はお問い合わせください。

※２）診断実行の限度数は、診断メニューにかかわらず月初～月末に 5 回です。
各診断を１つのみを実行した場合も１回カウントされます。各診断を同時に行った場合は

© Hitachi Systems, Ltd. 2024. All rights reserved.

１回のカウントになります。

※３）本サービスを使用した場合、以下の免責事項に同意したものとします。本免責事項は診断実行ページに記載しています。

【免責事項】
利用者は自らの責任及び判断において本サービスを利用するものとし、直接的・間接的を問わず 利用者が本サービスを利用したことにより生じたあらゆる損害、損失、責任、負担に対して 当社は一切責任を負わないものとします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.5 Joomla 簡易脆弱性診断機能

Web サイトを Joomla で構築されているお客様は、GRED の管理コンソール内からワンクリックで、現在使用している Joomla のバージョン情報やご利用のコンポーネント情報を検出し、検出されたバージョンおよびコンポーネントに脆弱性がないかをチェックすることができます。脆弱性ありと診断した場合、脆弱性のあるバージョンと脆弱性の内容を表示し、アップデートなどの情報を提供しているウェブサイトの URL 等、参照情報を表示します。

【使用方法】

© Hitachi Systems, Ltd. 2024. All rights reserved.

① 管理画面左上の☰をクリックし、「**解析内容の設定**」に遷移します。
② 左側の「**簡易脆弱性診断**」をクリックします。
③ 「**Joomla 診断**」にチェックを入れます。
④ 「**診断実行**」をクリックします。
⑤ 診断完了後、Joomla 診断結果のタブに結果が表示されます。

【ご注意事項】

※１）本診断の特性上、不正アクセス検知システム（サーバ監視ツールや、IPS/Firewall など）に不正なアクセス攻撃として検知される可能性がございます。診断を行う際は、事前に関連部署に対して脆弱性診断実施の了承、並びに本脆弱性診断サービスからのアクセスを一時的に監視対象から外していただく等のご対応をお願いいたします。
本ツールの IP アドレスを確認したい場合はお問い合わせください。

※２）本脆弱性診断が可能な回数は、月初～月末に 5 回です。
各診断を１つのみを実行した場合も１回カウントされます。各診断を同時に行った場合は１回のカウントになります。

※３）本サービスを使用した場合、以下の免責事項に同意したものとします。本免責事項は診断実行ページに記載しています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

【免責事項】
利用者は自らの責任及び判断において本サービスを利用するものとし、直接的・間接的を問わず利用者が本サービスを利用したことにより生じたあらゆる損害、責任、負担に対して当社は一切責任を負わないものとします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.6 リンク切れ検知機能

リンクが切れているページを検知しリスト表示します。リンク切れ検知の対象となるのは GRED のクローラが辿るリンクのみです。サーバから 404 エラー応答のあった URL をリンク切れとして検知します。表示されるのは最新の解析結果のみとなります。リンク切れを検知させるには、TOP 画面左メニューの「解析内容の設定」をクリックしオプションメニューの「リンク切れ検知設定」をクリックしてください。

① 管理画面左上の  をクリックし、「**解析内容の設定**」に遷移します。
② 「オプション」メニューから「**リンク切れ検知設定**」をクリックします。
③ 「リンク切れ検知設定」画面で「**有効**」を選択し、「**設定する**」ボタンをクリックします。

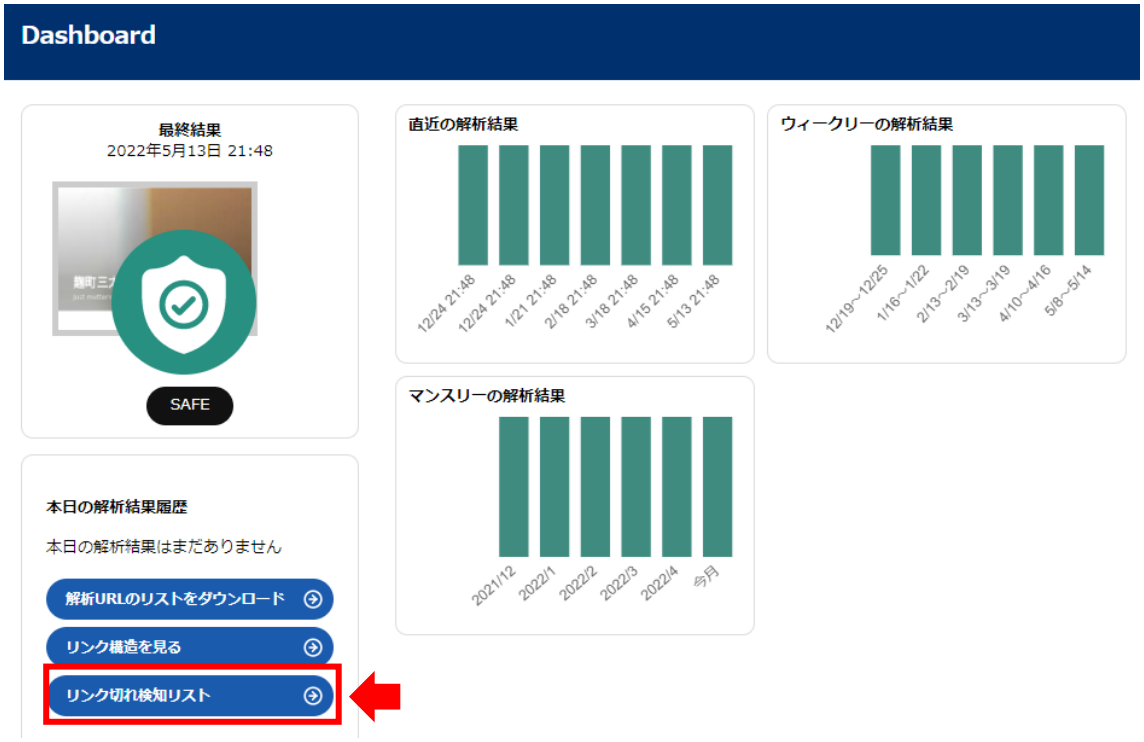
© Hitachi Systems, Ltd. 2024. All rights reserved.

リストの表示方法

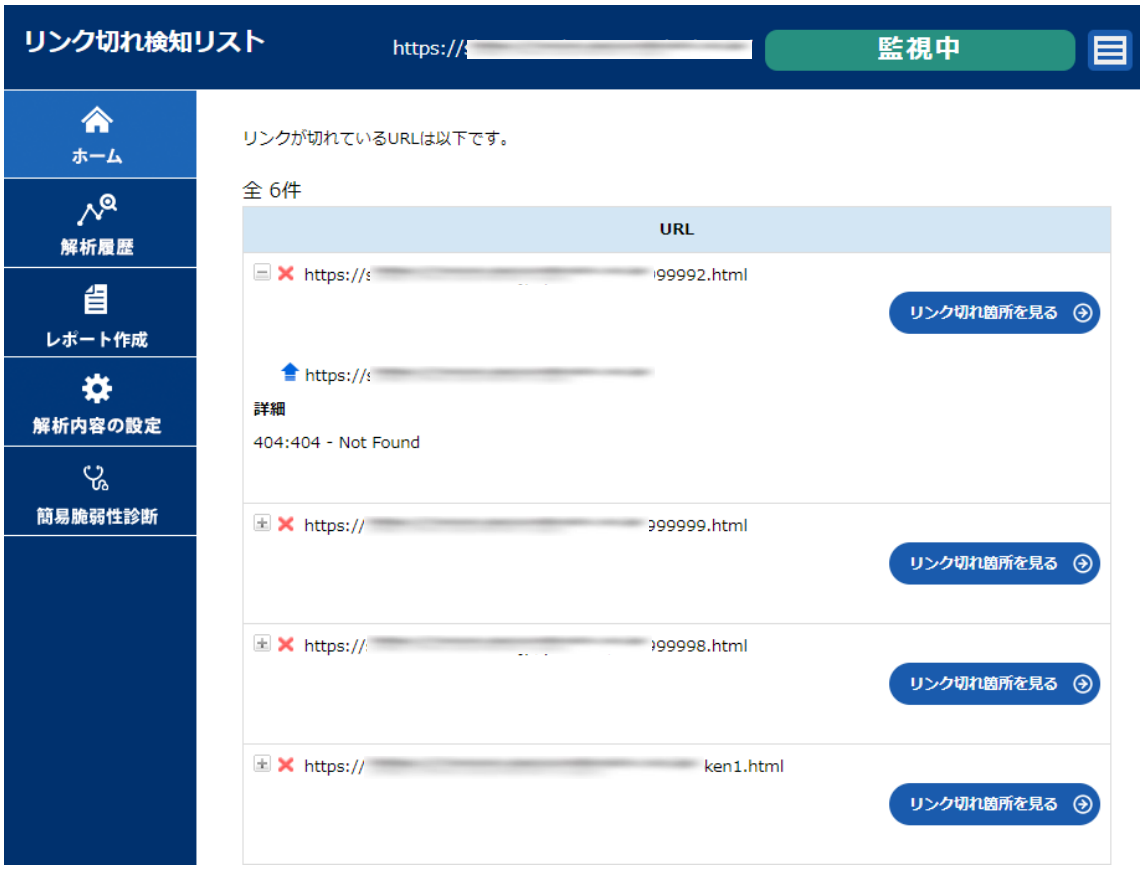
リンク切れ検知設定を有効にし、次回の解析以降、「リンク切れ検知リスト」が表示されます。

管理コンソール TOP 画面の下部にある「リンク切れ検知リスト」ボタンをクリック。

リンク切れを検知したリスト一覧ページにジャンプします。



© Hitachi Systems, Ltd. 2024. All rights reserved.



「＋」ボタンをクリックすると詳細情報を表示します。

❌　　・・・リンク切れの URL

⬆　　・・・リンク切れの URL がリンクされている URL

詳細　・・・サーバからの応答エラーコード

リンク切れ箇所を見る・・・リンク構造の可視化ページにジャンプします（「6.7 リンク構造可視化機能」参照）

© Hitachi Systems, Ltd. 2024. All rights reserved.

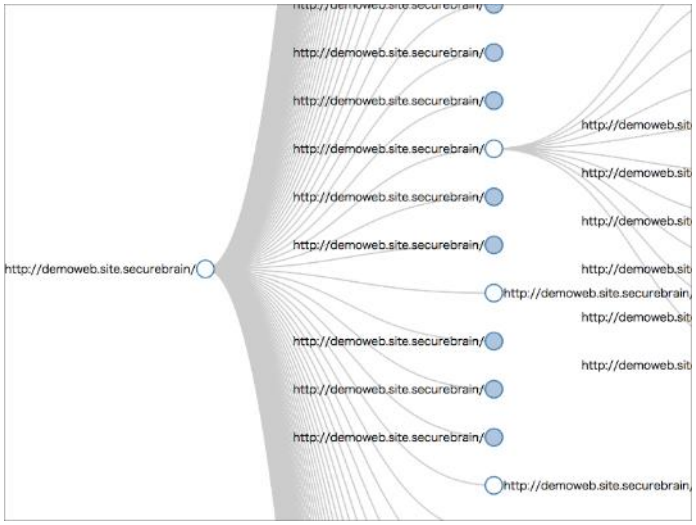
6.7 リンク構造可視化機能

リンク構造可視化機能（以下、本機能）は、GRED のクローラが改ざんの有無を検査するために収集した情報を元にサイトのリンク構造をツリー状に表示し可視化します。本機能を使用し改ざん検知箇所やアラート検知箇所、またリンク切れ検知箇所等を視覚的に理解していただくことで、影響範囲の把握や復旧の迅速化にお役立ていただけます。

リンク構造の表示方法

管理コンソール TOP 画面の下部にある「リンク構造を見る」ボタンをクリック。リンク構造の可視化ページにジャンプします。

TOP ページからリンクしているページをツリー状に表示します。



リンク構造のツリーはマウスで拡大・縮小・移動が可能です。

●をクリックするとそのページにリンクされているページ一覧が表示されます。

○表示の場合は、そのページにリンクされているページがありません。

© Hitachi Systems, Ltd. 2024. All rights reserved.

改ざん・クロスドメイン等を検知した場合の表示

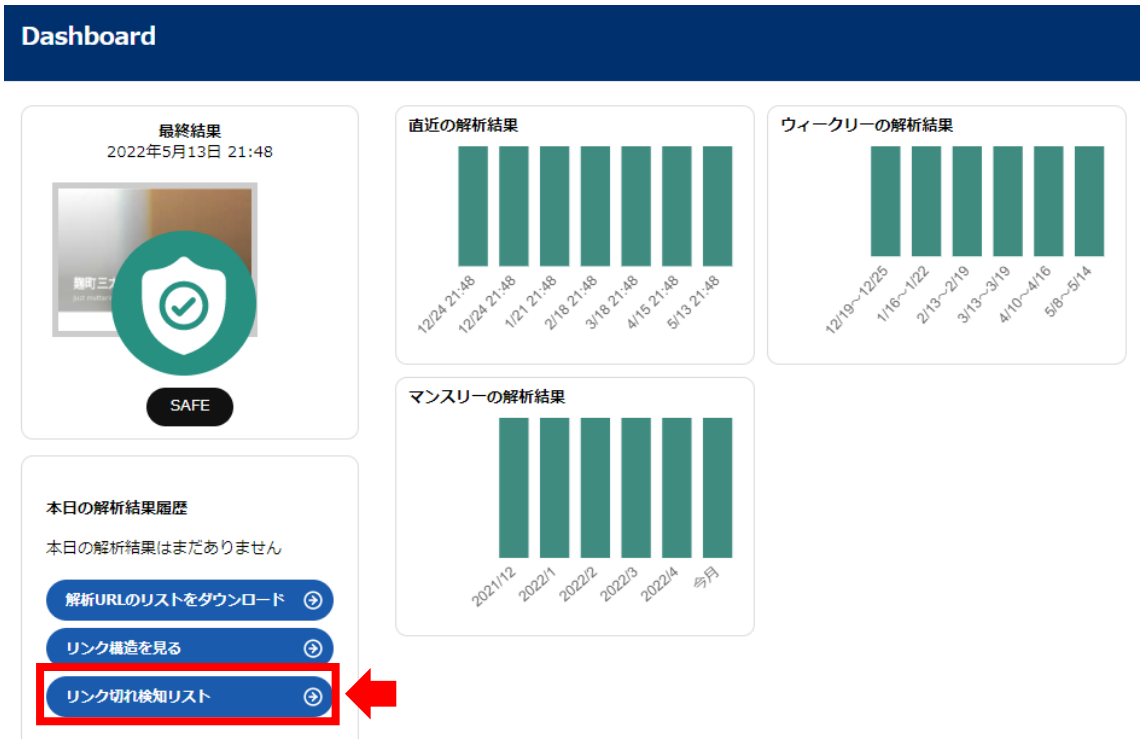
「検知箇所を表示」ボタンをクリックすると検知箇所がツリーの中心に表示されます。
改ざん検知した URL は赤色に変わります。クロスドメイン、表層解析等を検知した URL はオレンジに変わります。どちらの場合でも、URL の先頭のマルが赤になり点滅します。
検知箇所が複数ある場合は、緑の右矢印ボタンをクリックするとトップ URL に近い順に表示されます。

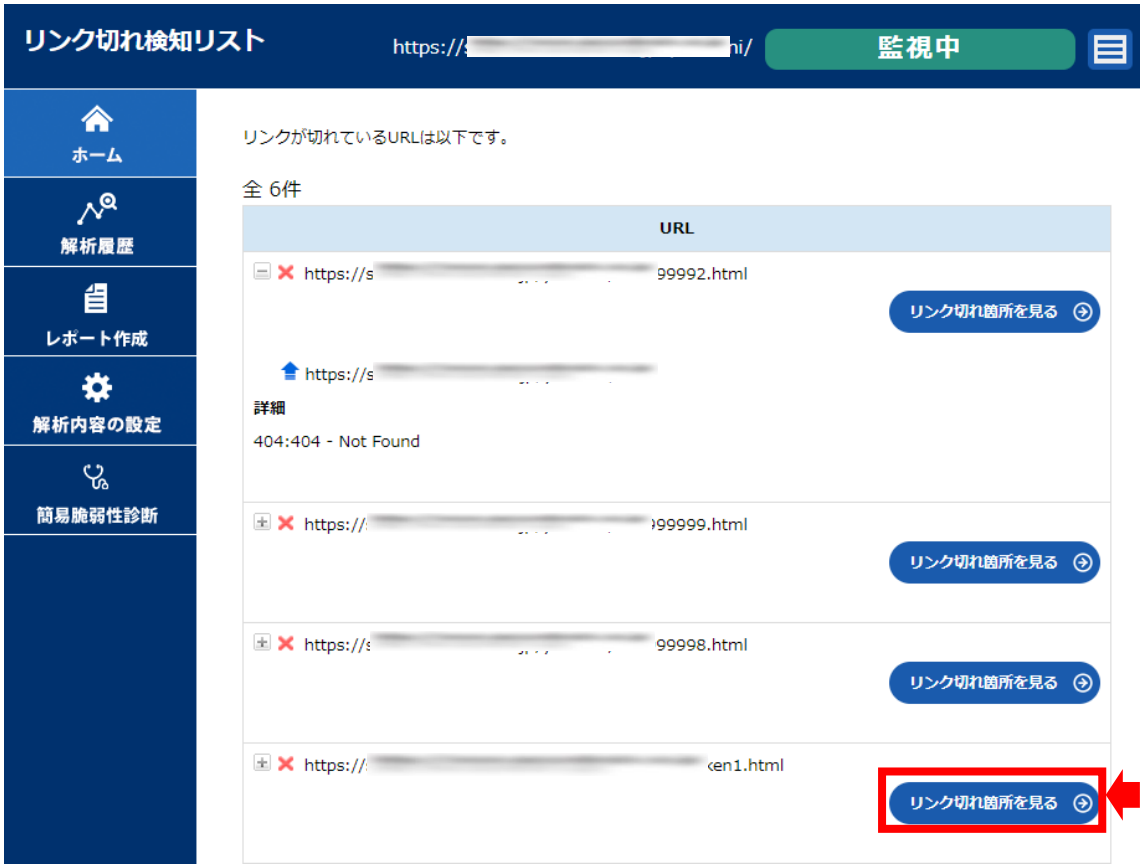
リンク構造の表示は改ざん箇所や内容を通知する詳細レポートからも可能です。管理コンソール TOP 画面のカレンダーのアイコンをクリックし、詳細レポートから「検知箇所を見る」をクリックしてください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

リンク切れを検知した場合の表示

管理コンソール TOP 画面の下部にある「リンク切れ検知」ボタンをクリック。
リンク切れを検知したリスト一覧ページにジャンプします。

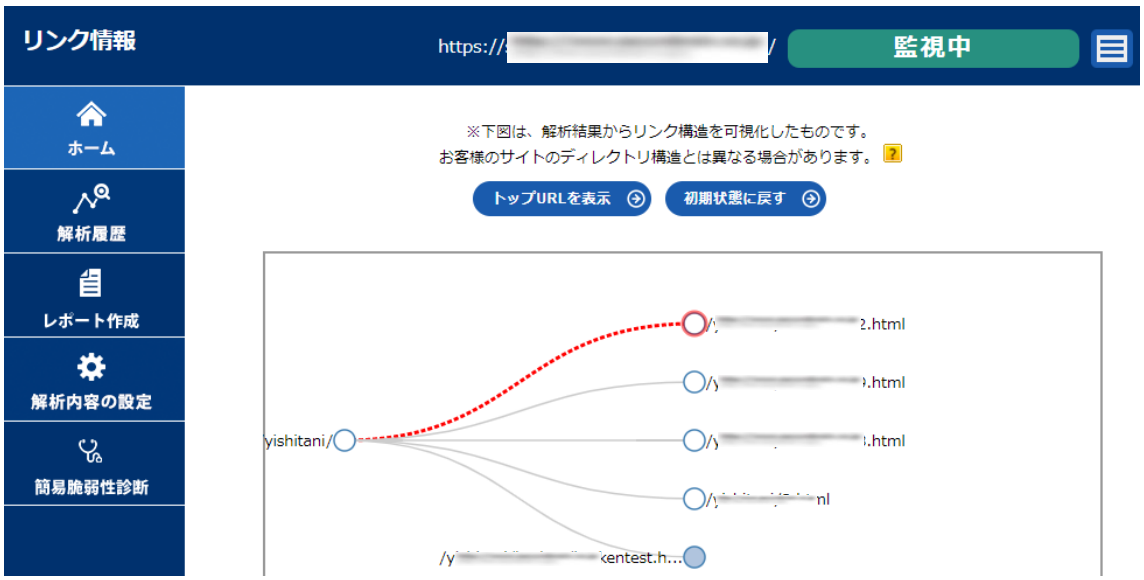




「リンク切れ箇所を見る」をクリックするとリンク構造の可視化ページにジャンプします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

リンク切れの部分は赤の点線で表示されます。リンク切れ URL の先頭のマルが赤になり点滅します。



リンク構造のツリーはマウスで拡大・縮小・移動が可能です。

●をクリックするとそのページにリンクされているページ一覧が表示されます。

○表示の場合は、そのページにリンクされているページがありません。

対応ブラウザ

Edge, Chrome, Firefox

【ご注意事項】

・本機能で表示されるリンク構造は、GRED の解析結果からリンク構造を可視化したものです。お客様のサイトのディレクトリ構造とは異なる場合があります。

・管理コンソール TOP 画面のカレンダーからリンク構造を可視化できる期間は、直近 1 週間です。

・可視化処理は JavaScript で動作しているため、処理時間はお使いの PC のスペックに依存します。

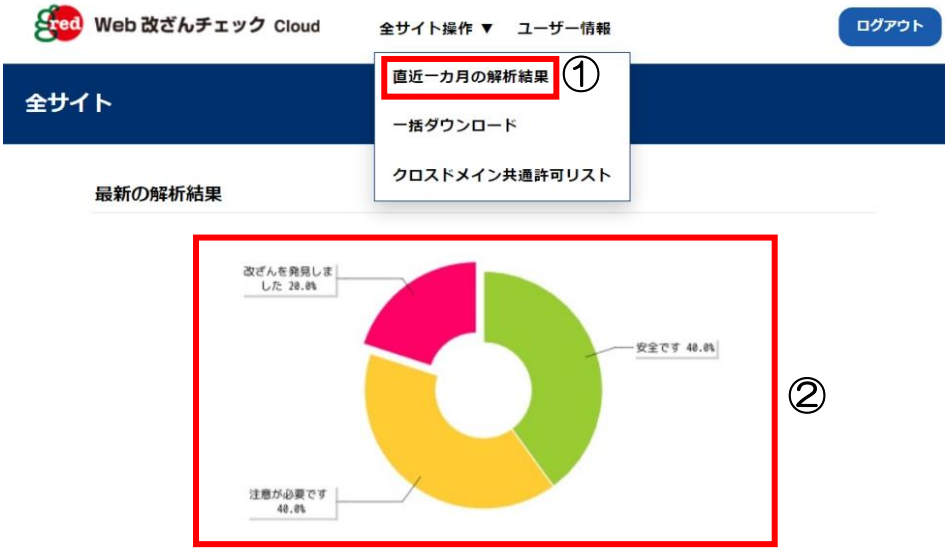
【免責事項】

利用者は自らの責任及び判断において本機能を利用するものとし、直接的・間接的を問わず 利用者が本機能を利用したことにより生じたあらゆる損害、損失、責任、負担に対して 当社は一切責任を負わないものとします。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.8 全サイトの状態

複数スケジュールを登録している場合、複数スケジュールの直近 1 ヵ月の解析情報を表示します。
※複数スケジュールが無い場合は、「全サイトの状態」ボタンは表示されません。
ヘッダーの「全サイト操作」の「直近一か月の解析結果」からアクセスできます。



	項目名	内容
①	直近一カ月の解析結果	全サイトの状態を表示します。
②	最新の解析結果	全スケジュールの最新の解析結果を円グラフで表示します。（緑色：正常、黄色：クロスドメインスクリプトの検知、赤色：改ざんの検知）
③	直近一ヵ月の検知（悪質/警告）	1 ヵ月以内の検知（悪質/警告）した、解析サイト名と、URL を表示します。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6.9 一括ダウンロード

複数スケジュールを登録している場合、複数スケジュールの解析 URL リストとレポートを一括ダウンロードできます。
※複数スケジュールが無い場合は、「一括ダウンロード」ボタンは表示されません。
ヘッダーの「全サイト操作」の「一括ダウンロード」からアクセスできます。

© Hitachi Systems, Ltd. 2024. All rights reserved.

	項目名	内容
①	一括ダウンロード	一括ダウンロード画面に遷移します。
②	スケジュールの絞り込み	複数スケジュールを条件により絞り込みます。
③	スケジュール一覧	スケジュール検索結果の一覧を表示します。 チェックボックスをチェックすることで、URL リストのダウンロード、レポートのダウンロードを行うスケジュールを選択出来ます。
④	URL リストのダウンロード	③で選択したスケジュールの、最新の解析履歴 URL リストをダウンロードします。 リストファイルと、インデックスファイルが ZIP 形式でダウンロード出来ます。
⑤	レポートのダウンロード 月次	③で選択したスケジュールの、月次（指定月一ヵ月分）レポートをダウンロードします。 レポート対象の年月を指定し、CSV ファイルでダウンロード出来ます。
⑥	レポートのダウンロード 日次	③で選択したスケジュールの、日次（指定日一日分）レポートをダウンロードします。 レポート対象の年月日を指定し、CSV ファイルでダウンロード出来ます。

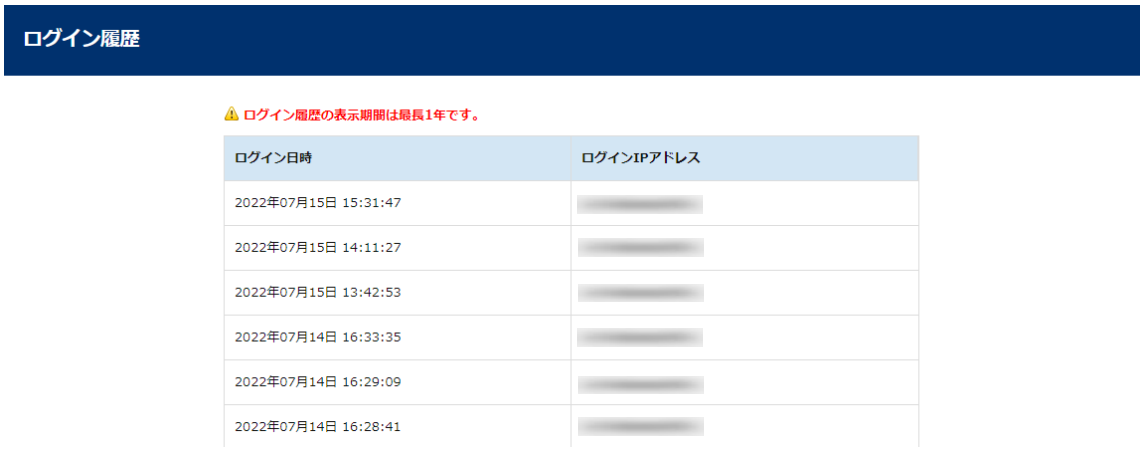
© Hitachi Systems, Ltd. 2024. All rights reserved.

6.10 パスワードをお忘れの場合

パスワードをお忘れによりログインできない場合に、ログインフォームの下にある『パスワードをお忘れの場合』リンクからパスワードを再設定することができます。あわせて二要素認証の設定を無効化することもできます。

6.11 ログイン履歴確認機能

これまでのログイン日時とそのログインを行った環境の IP を表示します。1 ページに最大 100 件が表示され、最長で過去 1 年分のログイン履歴を表示することができます。



© Hitachi Systems, Ltd. 2024. All rights reserved.

7. 申込み（新規申込・変更申請）

7.11 新規申込

所定の申込書にホスト名（FQDN：解析開始 URL）と解析 URL 数、お客様情報をご記入の上、提出してください。標準プランは、1 ホスト、1000URL、1 日 4 回解析になります。
標準プラン以外をご希望の場合は、購入元の代理店にご相談ださい。
新規申込が完了すると GRED システムから申し込み時に指定していただいたアラートメールアドレスに登録通知が届きます。

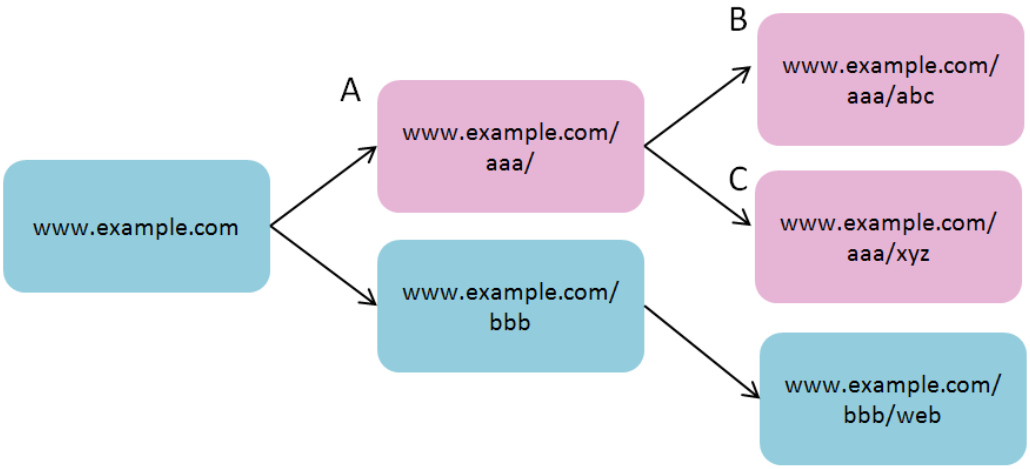
※所定の申込書は、巻末の「付録　新規申込/解約申請書」をご参照ください。
※管理画面の URL の詳細は、巻末の「付録 管理画面 URL」をご参照ください。

7.12 解析する URL 数、解析対象ホスト数

「GRED Web 改ざんチェック Cloud」の価格は、解析する URL 数、解析の対象とするホスト数によって変わります。まず、お客様の Web サイトの URL 数をご確認ください。URL 数が不明な場合は、購入元の代理店でカウントすることも可能ですので、お問い合わせください。

7.13 解析する URL の絞り込み(除外 URL の登録)

除外 URL の設定が可能です。解析 URL 数を調節する際にお使いいただけます。パス（ディレクトリ）指定を最大 100 個まで行う事ができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。**（この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.4 除外 URL の登録」をご覧ください。）**
※A(www.example.com/aaa/)を指定した場合、**B** と **C** も解析対象から除外されます。



© Hitachi Systems, Ltd. 2024. All rights reserved.

7.14 解析する URL の絞り込み(ウェブ解析対象階層の指定)

解析対象の階層数を指定する事により、不要なページのスキャンを防止いたします。
指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。**（この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.6** 監視の ON/OFF とウェブ解析対象階層の指定」**をご覧ください。）**

7.15 変更申請

所定の変更申請書に変更内容をご記入の上、提出してください。

※所定の変更申請書は、巻末の「付録　変更申請書」をご参照ください。

© Hitachi Systems, Ltd. 2024. All rights reserved.

付録　新規申込書

お客様にて、赤枠内をご記入ください。

お申し込みいただく前に、GRED Web改ざんチェック Cloudをご利用いただくための契約条件（https://www.gred.jp/saas/other/agreement.html）をよくお読みください。
お客様が本サービス申込みをいただいた時点で、これらの条項に同意されたとみなさせていただきますのでご了承くださいますようお願い申し上げます。

弊社は、お客様からご提供いただく個人情報を、弊社のプライバシーポリシー（https://www.hitachi-systems.com/privacy/index.html）を遵守した上で、弊社が企画・後援するイベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいますようお願い申し上げます。

GRED Web改ざんチェック Cloud　新規申請書

*1 希望日有りの場合：希望日の5営業日前迄に提出、最短希望「最短」と明記。

[1]申請内容　※赤枠部分は、記入必須項目です。

本申請書の提出が遅れた際は、ご希望日に添えない場合がございます。▼

お申し込み日	20　年　月　日	サービス開始希望日 *1	20　年　月　日	
契約種別（年額/月額/月額自動更新*2）	選択してください	基本契約数（基本ライセンス）	1ホスト・1,000URL	
解析回数（基本：1日4回）	1日4回	ホスト追加ライセンス 追加購入された数字を入力▸	0	ライセンス
ユーザID（ログインID）*3		合計ホスト数 入力不可▸	1	ホスト
アラート用メールアドレス*4・5		URL数追加ライセンス 追加購入された数字を入力▸	0	ライセンス
管理画面利用 ご担当者名*5		合計URL数 *7 入力不可▸	1,000	URL

【サービス解約ご希望の場合】解約希望月の1ヶ月前までに別途、解約申請書にて申請が必要となります。なお、料金の日割り計算は出来ないため、月中であっても解約利用月分の料金は発生しますのでご了承下さい。解約申請書がご必要な際は、パートナーセールス（partner_sales@securebrain.co.jp）までご連絡下さい。

*1：サービス開始日は、営業日の関係上、前倒しもしくは翌月のサービス開始日になる場合があります。納期につきましてはご販売会社へお問い合わせ下さい。

*2：【月額自動更新について】月額サービスはお客様が解約を1ヶ月前までに申請されない限り、自動継続として更新されます。

*3：ログインで使用するIDです。ユーザID（ログインID）は登録後、変更はできません。その為個人アドレスはお勧めしません。
使用可能な文字は8～50文字の半角英数字と、ダッシュ（-）、アンダースコア（_）、スラッシュ（/）、ピリオド（.）、アット・マーク（@）です。

*4：開通メール（サービス開始と管理画面のログイン情報のお知らせ）、並びに、改ざん発見時のアラートメール送信先となります。メールアドレスを1つご記入下さい。

*5：【サービス開始後のアラート用メールアドレス・管理画面利用ご担当者名の変更ご希望の方】
お客様管理画面（https://www.gred.jp/saas/）へログインいただき、「ユーザー情報の変更」からご自身での変更をお願いしております。尚、弊社へ変更連絡は不要です。
もし、現在のアラート用メールアドレスの登録情報がご退職者様のアドレス等の理由により受信出来ず、管理画面にログイン出来ない場合には、
サポートセンター〈E-mail：biz_support@securebrain.co.jp〉（https://www.securebrain.co.jp/support/index.html）へ連絡して下さい。ご希望のアドレスへ変更致します。

[2]ホスト（解析開始URL）とURL数

	ホスト（解析開始URL）*6　※必ず　https://　（又はhttp://）　からご記入をお願い致します。	URL数
No.	（記入例）https://www.securebrain.co.jp	（例）1000
(1)		
(2)		
(3)		
(4)		
(5)		
(6)		
(7)		
(8)		
(9)		
(10)		
	合計URL数（セルM12参照）　入力不可▸ *7：複数のホストがある場合は、「合計URL数」内に納まるように、数を割り当てください。	0
備考		

*6-1：ドメインが同一の場合でも、サブドメインが異なる場合は別ホストとなりますので、ご注意下さい。（例）『www.securebrain.co.jp』と『info.securebrain.co.jp』は、別ホスト扱い。

*6-2：FQDNが同一の場合でも、解析開始URLが異なる場合は別ホスト扱いとなりますので、その分のライセンスの追加が必要になります。
（例）『https://www.securebrain.co.jp/』と『https://www.securebrain.co.jp/eng/』は、別ホスト扱い。

[3]お客様情報　◎ご契約者が管理画面利用者も兼ねられる場合は、管理画面利用者の欄には「同左」とご記入いただいても結構です。

	ご契約者（サービスの購入と管理をされる方）	管理画面利用者（GREDシステムを利用し、サポートを受けられる方）
■会社名		
■ご所属部署/役職名		こちらの利用者は、上方記載*5と同一の方となります。 担当者名・メールアドレスの変更方法は*5を参照下さい。 尚、グレー部分の変更におきましては、 弊社への変更連絡は不要でございます。
■ご担当者名		
■電子メールアドレス		
■電話番号		
■備考　ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、エンドユーザー名をご記載下さい		

[4]パートナー情報

	パートナー（販売1次店）	パートナーの代理店（販売2次店）
■会社名		
■ご所属部署/役職名		
■ご担当者名		
■電子メールアドレス*9（更新案内連絡先）		社名以外、申請不要
■電話番号		
■備考欄　注文番号（PO番号）等、必要に応じてご記入下さい		

*9：月額自動更新以外は、更新案内メールの送信にも利用させていただきますので、案内メールの受取先メールアドレスをご連絡ください。3アドレスまで可。

SBC(20231211)

© Hitachi Systems, Ltd. 2024. All rights reserved.

付録　変更申請書

弊社は、お客様からご提供いただく個人情報を、弊社のプライバシーポリシー(https://www.hitachi-systems.com/privacy/index.html)を遵守した上で、弊社が企画・後援するイベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいますようお願い申し上げます。

GRED Web改ざんチェック Cloud　変更申請書

[1]サービス内容　▼下記赤枠、ご記入ください。

お申し込み日	年　月　日	基本ライセンス(1ホスト・1000URL)	変更前	変更後
変更希望日*3	年　月　日	ホスト追加ライセンス 追加購入された数字を入力▸	0	0
契約種別 (年額/月額/月額自動更新)	選択ください	合計ホスト数 入力不可。自動計算▸	1	1
ユーザID (ログインID) *1:ユーザーIDは変更できません。		URL追加ライセンス 追加購入された数字を入力▸	0	0
アラート用メールアドレス*2(任意)		合計URL数 *4 入力不可。自動計算▸	1,000	1,000
管理画面利用　ご担当者名*2(任意)		解析回数(基本:1日4回)	要選択	要選択

*2:項目を変更方法▸管理画面(https://www.gred.jp/saas/)へログイン後「ユーザー情報の変更」から、**お客様ご自身で変更をお願い致します。**尚、弊社への変更連絡は不要です。
もし、現在のアラート用メールアドレスの登録情報がご退職者様のアドレス等の理由により受信出来ず、管理画面にログイン出来ない場合には、
サポートセンター(E-mail:biz_support@securebrain.co.jp)(https://www.securebrain.co.jp/support/index.html)へ連絡して下さい。ご希望のアドレスへ変更致します。

*3:**希望日有りの場合:希望日の5営業日前迄**に提出、**最短希望の場合:「最短」**と明記下さい。内容に不備がある場合、再提出等、受理する迄にリードタイムを要する為、余裕をもって申請下さい。

[2]ホスト(解析開始URL)とURL数の設定 *5

*5-1. ホスト(解析開始URL)は必ずhttps://(又はhttp://)からご記入下さい。

*5-2. 改ざん時切り替え機能をご利用の場合、開始URLを変更される場合は、変更後のページに改ざん時切り替え機能のタグを挿入して下さい。

*5-3. ドメインが同一の場合でも、サブドメインが異なる場合は、別ホスト扱いとなりますので、追加ライセンスが必要になります。
(例)『www.securebrain.co.jp』と『info.securebrain.co.jp』は、別ホスト扱い。

*5-4. FQDNが同一の場合でも、解析開始URLが異なる場合は、別ホスト扱いとなりますので、その分のライセンスの追加が必要になります。
(例)『https://www.securebrain.co.jp/』と『https://www.securebrain.co.jp/eng/』は、別ホスト扱い。

【重要:課金月について】日割り計算は行っていない為、通常、下記の通りです。
・ホスト数やURL数を減少する場合は、**翌月より減額**
・ホスト数やURL数を追加する場合は、**当月より増額**
※上記対応が難しく、日程や課金調整が必要な場合はお問合せ下さい。

▼「区分*6」を選択して下さい。

変更	・**解析開始URL**の変更の場合:**上書き変更**され、解析履歴は引き継がれます。 ・**URL数**の増減の場合:ご希望のURL数を明記下さい。
追加(ホスト)	・新たなホストNo.に、解析開始URL明記下さい。**「新規ホスト」として追加**します。 ※削除依頼したホストNo.欄に追記はご遠慮下さい。
変更無	・対応無し。 ※変更前URLをそのまま、変更後欄へ明記下さい。
削除	・**変更希望日(当日)、又は5営業日以内に削除**されます。 **【削除依頼時の注意】** ・行削除・詰めて明記はせず、「削除」選択下さい。左右対称でなくなる為。 ・**URLの削除後は、解析履歴の閲覧が出来なくなる**為、もし履歴が必要な際は、変更希望日前迄に管理画面の「解析履歴」より事前DLをお願い致します。

変更前					区分 *6	変更後			
ホストNo.	ホスト(解析開始URL) *5			URL数		ホスト(解析開始URL) *5			URL数
1					要選択				
2					要選択				
3					要選択				
4					要選択				
5					要選択				
6					要選択				
7					要選択				
8					要選択				
9					要選択				
10					要選択				
	合計ホスト数	0	合計URL数 *4:セル「N8」参照 複数ホストの場合、「合計URL数」内で割振り下さい	0		合計ホスト数	0	合計URL数 *4:セル「O8」参照 複数ホストの場合、「合計URL数」内で割振り下さい	0
	備考								

[3]お客様・[4]パートナー情報に変更がある場合、変更されたい部分のみ、ご記入ください。

▼変更箇所にチェック		ご契約者 (サービスの購入と管理をされる方)	管理画面利用者 (GREDシステムを利用し、サポートを受けられる方)
□	会社名		
□	ご所属部署/役職名		こちらの利用者は、上方記載*2と同一の方となります。 担当者名・メールアドレスの変更方法は*2を参照下さい。 尚、グレー部分の変更におきましては、 弊社への変更連絡は不要でございます。
□	ご担当者名		
□	電子メールアドレス		
□	電話番号		
□	備考 ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、E/U名をご記載下さい		

▼変更箇所にチェック		パートナー(販売1次店)	パートナーの代理店(販売2次店)
□	会社名		
□	ご所属部署/役職名		社名以外、申請不要
□	ご担当者名		
□	電子メールアドレス*8 (更新案内連絡先)		
□	電話番号		
□	備考 注文番号(PO番号)等、必要に応じてご記入下さい		

*8:月額自動更新以外は、更新案内メールの送信にも利用させていただきますので、案内メールの受取先メールアドレスをご連絡ください。3アドレスまで可。

SBC(20231211)

© Hitachi Systems, Ltd. 2024. All rights reserved.

付録　解約申請書

お申し込みいただく前に、GRED Web改ざんチェック Cloudをご利用いただくための契約条件（https://www.gred.jp/saas/other/agreement.html） をよくお読みください。
お客様が本サービス申込みをいただいた時点で、これらの条項に同意されたとみなさせていただきますのでご了承くださいますようお願い申し上げます。

弊社は、お客様からご提供いただく個人情報を、弊社のプライバシーポリシー（https://www.hitachi-systems.com/privacy/index.html）を遵守した上で、弊社が企画・後援する
イベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいますようお願い申し上げます。

GRED Web改ざんチェック Cloud　解約申請書

[1]申請内容　※赤枠内を埋めていただきます様お願い致します。

解約申請日*1	20　年　月　日	**サービス解約希望月*2** （最終課金月）	20　年　月
解約理由 今後のサービス向上に役立てる為、 お聞かせいただけますと幸いです。			

*1：解約希望月の**1ヶ月前まで**に申請が必要となります。

*2：解約希望月の**翌月第1営業日**に、解約のお手続き(サービス停止)させていただきます。
（例）解約希望月：2022年10月の場合、2022年11月1日に解約処理となります。
月途中の解約をご希望の方は、日にち迄ご記入ください。解約希望日で停止をさせていただきます。
尚、解約日が月途中でも、料金の日割り計算は出来ませんのでご了承ください。
稀に年末年始・GW等、弊社都合で作業が遅れることもございますが、課金は解約月迄となりますのでご安心下さい。
もし遅れる場合、作業日については、内容を確認後、担当者よりご連絡いたします。

[2]現在ご提供中のサービス内容*3

ユーザID（ログインID）	
アラート用メールアドレス(任意)	
管理画面利用 ご担当者名(任意)	

*3：URLの解析履歴に関しましては、解析日時から1年経過したURLごとに、自動で削除されます。
履歴を残したい場合には、管理画面の「解析履歴」より、ダウンロードをお願い致します。

[3]お客様情報　◎ご契約者が管理画面利用者も兼ねられる場合は、管理画面利用者の欄には「同左」とご記入いただいても結構です。

	ご契約者 （サービスの購入と管理をされる方）	**管理画面利用者** （GREDシステムを利用し、サポートを受けられる方）
■会社名		
■備考　ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、エンドユーザー名をご記載下さい。		

[4]パートナー情報

	パートナー（販売1次店）	**パートナーの代理店**(販売2次店)
■会社名		
■備考		

この度は、弊社サービスをご利用いただき、誠にありがとうございました。
今後とも、サービスの向上に努めてまいりますので、また機会がございましたら株式会社セキュアブレインをよろしくお願いいたします。

SBC(20231211)

© Hitachi Systems, Ltd. 2024. All rights reserved.

付録　管理画面 URL

管理画面 URL は以下の通りです。

管理画面 URL	https://www.gred.jp/saas/

© Hitachi Systems, Ltd. 2024. All rights reserved.

付録　アラートメールサンプル

アラート通知メールのサンプルは以下の通りです。

1	改ざん検知時
2	Top ページのヘルスチェック検知時
3	見た目変化検知時
4	クロスドメインスクリプト検知時
5	EXE 解析検知時
6	タグ変化検知時/JavaScript 変化検知時
7	週間レポート
8	お知らせ通知

© Hitachi Systems, Ltd. 2024. All rights reserved.

1. 改ざん検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]Web 改ざんの可能性を検知
本文サンプル	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web ページに Web 改ざんの可能性を発見しました。 Web 改ざんが発見された URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 改ざんを検知した Web ページの詳細確認は、必ず下記の Web サイトからご確認下さい。 監視中の Web サイト： 検知 URL： 内容：脆弱性を持つサイトの疑いのあるコンテンツが発見されました このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

2. Top ページのヘルスチェック検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]Web のコンテンツが見つかりません
本文	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web コンテンツにアクセスできません。 Web サイトの確認をお願いします。 解析開始 URL： 検知 URL： 内容：Web サイトでエラーが発生しています。 詳細： 詳細については下記 Web サイトをご参照下さい。 ■よくあるエラーコード 403 - Forbidden：適切に権限がついているか確認してください。 ※ファイルパーミッション・アクセス制限など 404 - Page Not Found：ページが見つかりません。 コンテンツが正常にアップされているか確認してください。 今後この警告を停止する場合は、ログイン後、[解析内容の設定]-[基本設定]から監視の ON・OFF から OFF を選択してください。 このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

3. 見た目変化検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]TOP ページの見た目が変化した可能性を検知
本文	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web サイトで TOP ページの見た目が変化した可能性を検知しました。 TOP ページの見た目の変化を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 Web ページの詳細は、必ず下記の Web サイトからご確認ください。 監視中の Web サイト： 検知 URL： 内容：見た目変化の可能性の疑いのあるコンテンツが発見されました このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

4. クロスドメインスクリプト検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]クロスドメインスクリプトを検知
本文	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web ページに新たなドメインから実行する下記のクロスドメインスクリプトを発見しました。 このスクリプトが正規に追加されたスクリプトの場合は必ず、[解析内容の設定]-[クロスドメイン設定]-[クロスドメイン検知]の設定画面：「許可リスト」にクロスドメインの登録を行ってください。 Web 改ざんが発見された URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 改ざんを検知した Web ページの詳細確認は、必ず下記の Web サイトからご確認下さい。 監視中の Web サイト： 検知 URL： 内容：クロスドメインスクリプトの疑いのあるコンテンツが発見されました 検知経路： このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

5. EXE 解析検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]ファイルのマルウェア類似挙動の可能性を検知
本文	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web ページにリンクされたファイルのマルウェア類似挙動の可能性を検知しました。 マルウェア類似挙動の可能性を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 Web ページの詳細は、必ず下記の Web サイトからご確認ください。 監視中の Web サイト： 検知 URL： 内容：怪しいファイルの疑いのあるコンテンツが発見されました この検知はマルウェアとして検知するものではなく、あくまでもマルウェア類似の動きを検知したものです。 検知したファイルが正常なものである場合、ホワイトリストに登録することで以降の検知を回避することができます。 ホワイトリストに登録するかどうかは、自社にて判断ください。 このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

6. タグ変化検知時/JavaScript 変化検知時

送信元	gred@service.securebrain.co.jp
件名	[GRED]Web コンテンツデータが変化した可能性を検知
本文	「GRED Web 改ざんチェック」からのお知らせです。 監視中の Web ページで Web コンテンツデータが変化した可能性を検知しました。 Web コンテンツデータの変化を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 Web ページの詳細は、必ず下記の Web サイトからご確認ください。 監視中の Web サイト： 検知 URL： 内容：スクリプト/リンクタグ変化の疑いのあるコンテンツが発見されました このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。 本メールは、送信専用メールアドレスからお送りしています。

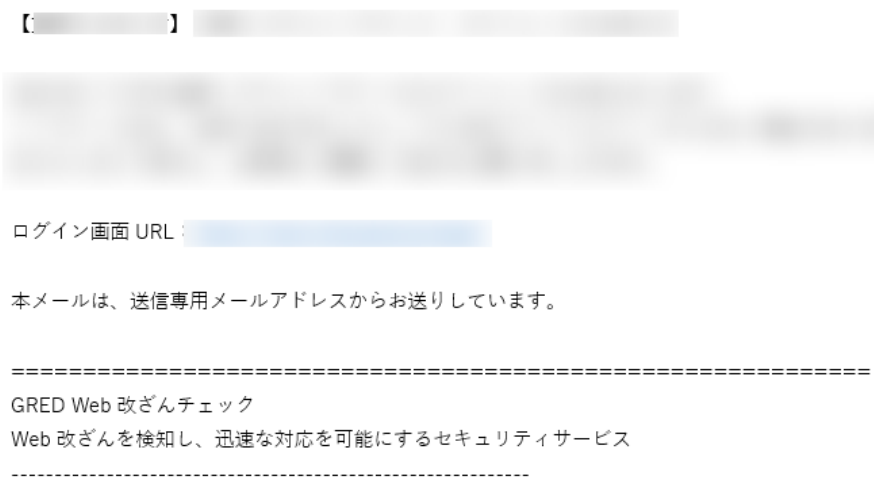
© Hitachi Systems, Ltd. 2024. All rights reserved.

7. 週間レポート

送信元	gred@service.securebrain.co.jp
件名	[GRED]週間レポート
本文	[redacted]様、 いつもGREDの「Web改ざんチェック」サービスをご利用いただきましてありがとうございます。 本サービスはWeb改ざんを検知し、迅速な対応を可能にするセキュリティサービスです。 今週のレポートを送付させていただきます。 ---------- 今週のWeb改ざんチェックのレポート ---------- レポート期間：[redacted] 監視中のWebサイト：[redacted] 対象ドメイン： １週間でチェックした回数：2回 改ざんを通知した回数：0回 警告を通知した回数：1回 貴社のWebページ数(平均)：3ページ ---------- 詳細な情報や、週間レポート送信サービスの設定を変更する場合は、gred セキュリティサービスにログインして「ユーザ情報の変更」で行ってください。 https://www.gred.jp/saas/ このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。

© Hitachi Systems, Ltd. 2024. All rights reserved.

8. お知らせ通知

送信元	gred@service.securebrain.co.jp
件名	GRED Web 改ざんチェックからのお知らせ【${CATEGORY}】
本文	

通知メールの件名の${CATEGORY}は、お知らせの種別により変わります。

重要なお知らせ	：	システムメンテナンス等のお知らせメールの場合
ご案内	：	新機能の追加等の案内メールの場合
障害	：	障害が発生時の通知メールの場合

© Hitachi Systems, Ltd. 2024. All rights reserved.